

A close-up, high-contrast photograph of a black cat's face. The cat's eyes are wide open and glow with a bright, yellow-green light, set against the dark, almost black fur of its face. The lighting is dramatic, highlighting the texture of the fur and the intensity of the eyes.

RouterOS v6.x

MikroTik KungFu Kitab 1

Rendra Towidjojo

An Acknowledge

Terima kasih untuk Allah, SWT atas semua Rahmat-Mu, Anugrah-Mu dan jalan yang Engkau pilihkan.

Ayahanda James Nurtanio, Kakanda Nurhayadi, Kedua Maha Guru saya di KailiNetwork: Mr. Denny Kristna dan Mr. Daniel KailiNet... terima kasih juga atas koneksi Internet gratisnya ☺. Guru CCNA saya : Mr. Taufik Muhammad, Mr. Yayat, Mr. Arief Budiman. Teman-teman seperjuangan di STMIK Adhi Guna Palu, AMIK Tri Dharma Palu, STMIK Bina Mulia Palu.

Para Admin IlmuJaringan(dot)Com yang banyak menemani saya berjuang : Kakanda Abu Fatimah (atas diskusi dan sarannya), Bro Budy Tan (yang sudah bersedia menjadi Technical Review bagi buku ini), Bro Aman Ozx (atas design covernya....you are the kungfu master), Bro Katiman Bayu (atas pinjaman remote akses ke Warnet CintaNet), Bro Nizam, Bro Adithya Erlangga, Bro Naim, Bro Riki. Rekan-rekan di IJC : Bro IR Scout (atas pinjaman RB751U-nya), Bro Aprisman (atas pinjaman halaman login MorokoaNet), Bro Hendra Surya (atas resumenya ttg HotSpot), Putu, Octo, Ardan, Okta, Kang Irwandhi, Kang Agus Sasmito, Kang Diaz dan rekan-rekan yang tidak mungkin lagi saya sebutkan satu per satu.

Terima kasih yang sebesar-besarnya untuk Mas S'to dan para Admin Jasakom yang sudah bersedia menerbitkan buku ini, dan tentunya terima kasih bagi Anda semua yang sudah bersedia membeli buku ini.

Preface

Alhamdulillah, Puji Syukur kehadiran Allah, SWT, buku **MikroTik Kungfu Kitab 1** akhirnya bisa selesai juga. Buku ini saya tulis dengan maksud memberikan pengetahuan awal bagi siapa saja yang ingin menggunakan Router MikroTik. Buku ini dapat digunakan bagi Anda yang benar-benar baru mengenal Router MikroTik. Anda yang sudah sering menggunakan Router MikroTik pun dapat menggunakan buku ini, ada banyak pembahasan konfigurasi di buku ini yang selama ini jarang dibahas dan diterapkan.

Walaupun berisi konfigurasi-konfigurasi Router MikroTik, namun saya tetap membahas dasar teori yang berkaitan dengan konfigurasi tersebut. Ini saya maksudkan, agar setelah membaca buku ini, Anda dapat mengembangkan sendiri konfigurasi Router MikroTik sesuai dengan kondisi jaringan yang Anda hadapi. Adapun acuan dari materi di buku ini adalah bahan sertifikasi MTCNA (MikroTik Certified Network Associate) maupun konfigurasi-konfigurasi yang ada di Wiki MikroTik (wiki.mikrotik.com).

Konfigurasi-konfigurasi yang di bahas di buku ini adalah konfigurasi dasar. Konfigurasi lanjutan yang lebih mendalam akan saya bahas pada buku selanjutnya. Bukankah manusia itu harus merangkak dulu, untuk kemudian belajar berdiri, berjalan kemudian berlari. Pemahaman yang baik pada konfigurasi dasar akan memudahkan Anda untuk melakukan konfigurasi lanjutan.

Akhir kata, semoga buku ini bermanfaat bagi kita semua dalam menerapkan konfigurasi Router MikroTik secara bijak. Salam KungFu !!!

Rendra Towidjojo
(rtowidjojo@gmail.com)

MikroTik Kung Fu Kitab 1 (Edisi 2018)

Bab 01 Pengenalan MikroTik Router

Untuk Apa Saja Router MikroTik Ini?

Sebagai Internet Gateway bagi LAN

Sebagai Access Point (Indoor/Outdoor)

Sebagai Intermediary Device (Routing)

Bagaimana Mendapatkan Router MikroTik ?

Instalasi MikroTik RouterOS

Lisensi RouterOS

Versi RouterOS

Apa Yang Harus Menjadi Modal Anda

Skenario Jaringan

Perintah Router MikroTik

Mempersiapkan Router MikroTik

Prosedur Reset

Login ke Router MikroTik

Konfigurasi Bridging

Bab 02 Konfigurasi Dasar

Persiapan Konfigurasi

Konfigurasi Interface

Mengganti Nama Interface

Menonaktifkan Interface

Konfigurasi Internet Gateway

Topologi

Konfigurasi IP Address

Konfigurasi Default Route

Konfigurasi DNS Server

Masquerade

Konfigurasi Tambahan

Konfigurasi User

Identity

NTP (Network Time Protocol) Client

Bab 03 Dynamic Host Configuration Protocol (DHCP Server)

Konfigurasi Dasar

Pengujian

Static Mapping

Pengamanan dengan DHCP Server

Bab 04 Firewall (Filter)

Konsep Dasar Firewall

Chain

Action

Top to Bottom

Topologi

Filter Berdasarkan IP Addresss

Parameter src-address

Parameter time

Best Practice

Filter Services

Filter HTTP dan HTTPS

Filter Domain Name System (DNS)

Best Practice

Filter Website

Filter dengan Content

Filter dengan L7 Protocol

Best Practice

Bab 05 Wireless Network

Konsep Dasar Wireless Network

Mode

Band

Frequency

SSID

Konfigurasi Dasar

Topologi

Konfigurasi Parameter Wireless

Konfigurasi IP Address

Pengujian dan Monitoring

Security Key

- Virtual Access Point
 - Topologi
 - Konfigurasi Virtual Access Point
 - Security Key
- Perluasan Jaringan Wireless
 - Topologi
 - Konfigurasi Internet Gateway
 - Konfigurasi Access Point
 - Monitoring

Bab 06 Hotspot Server

- Konfigurasi Dasar
- Manajemen User
 - Menambahkan User
 - Mengenal User Profile
- Monitoring
- Halaman Login
- Skenario Lain

Bab 07 Bandwidth Management

- Konsep Dasar Manajemen Bandwidth
 - CIR dan MIR
 - Queue pada Router MikroTik
 - Inner Queue dan Leaf Queue
- Konfigurasi Dasar
 - Topologi
 - Konfigurasi Simple Queue
 - Pengujian Awal
- Pengujian
 - Bandwidth Test
 - speedtest.net
 - Torch
- Multiple Network
 - Topologi
 - Konfigurasi
- Per Connection Queue (PCQ)
 - Konsep Dasar PCQ

Skenario 1

Skenario 2

Bab 08 Switch Chip

Prinsip Dasar Switch Chip

Router vs Switch

Switch Chip pada RouterBoard

Penerapan Switch Chip

Skenario 1

Skenario 2

Bab 09 Manajemen Router

Backup dan Restore

Backup

Restore

Export

Manajemen Service

Manajemen System

Enable/Disable Package

Download Package

Menambahkan Package

Menghapus Package

Upgrade RouterOS

Bab 10 Monitoring

Monitoring Hardware

Membaca Log

Monitoring User

Monitoring Bandwidth (Graph)

Mengaktifkan Graph

Membaca Graph

Bab 01

Pengenalan MikroTik Router

Yaa !!!, MikroTik !!!, siapa sih “anak IT” yang tidak mengetahui benda ini? Kalaupun sampai saat ini belum pernah melihat benda ini, paling tidak Anda sebagai “anak IT” (khususnya “anak jaringan”) pernah mendengarnya. MikroTik dikenal luas sebagai router. Router itu sendiri adalah perangkat yang digunakan untuk menghubungkan beberapa jaringan komputer (computer network). Dan Router MikroTik paling banyak digunakan untuk menghubungkan jaringan lokal (LAN) ke Internet. Pada jaringan yang lebih kompleks, Router digunakan untuk memilihkan jalan bagi paket data untuk mencapai komputer tujuan.

Router merupakan perangkat jaringan yang cerdas. Router bisa memahami betul bagaimana mengirimkan data dari satu jaringan ke jaringan lain. Jarang sebuah router salah menyampaikan paket data. Kembali lagi ke Router MikroTik yang ternyata merupakan router yang memiliki fitur sangat lengkap, mudah dikonfigurasi dan tentunya harganya yang murah. Walaupun ada juga Router MikroTik yang bisa seharga sepeda motor ataupun seharga sebuah mobil bekas.

Khusus untuk buku ini, akan dibahas bagaimana sebuah Router MikroTik dapat digunakan untuk membagi-bagi koneksi Internet ke beberapa komputer pengguna (user). Komputer-komputer tersebut dapat berupa PC Desktop yang menggunakan kabel jaringan (UTP) maupun Laptop/Smartphone yang menggunakan koneksi jaringan nirkabel (wireless). Tentu saat akan membagi koneksi Internet harus diperhatikan beberapa hal, layaknya jika ingin membagi sepotong kue yang Anda miliki, tentu Anda ingin membaginya dengan adil. Namun dalam kondisi tertentu, kadang-kadang Anda tidak menginginkan seseorang memakan kue milik Anda kan? ☺ Inilah yang akan dibahas pada buku ini, membagi-bagi koneksi Internet secara adil, merata dan berperikemanusiaan ☺.

Perlu diingat bahwa buku ini adalah buku bagi para pemula. Buku ini diperuntukkan bagi Anda yang baru mulai menggunakan Router MikroTik. Dan setelah Anda menguasai pembahasan dalam buku ini, maka Anda bisa lagi membaca buku-buku MikroTik Kung Fu seri berikutnya maupun buku yang lain tentang Router MikroTik.

Untuk Apa saja Router MikroTik ini?

Ini pertanyaan menarik, karena banyak di antara kita kadang-kadang tidak menggunakan Router MikroTik secara maksimal. Melihat pada uraian sebelumnya yang menyebutkan bahwa router adalah perangkat jaringan yang “pintar”, maka Router akan memiliki banyak peran dalam jaringan komputer. Ini karena Router MikroTik itu sendiri memiliki banyak fitur. Fitur-fitur inilah yang membuat Router MikroTik dapat mengambil peran yang lebih banyak dalam jaringan.

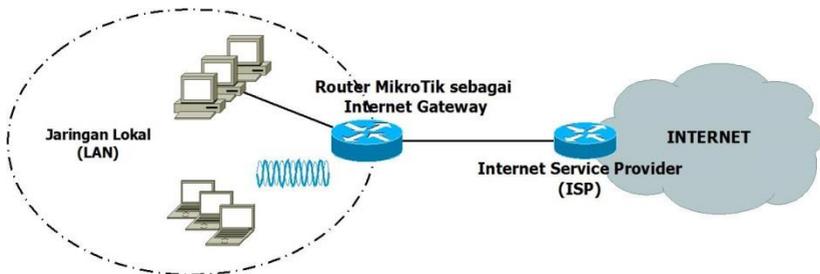
Pada sub bab ini, akan diberikan beberapa contoh implementasi Router MikroTik di lapangan. Contoh-contoh inilah yang paling sering diterapkan.

Sebagai Internet Gateway bagi LAN

Inilah peran yang paling banyak dimainkan oleh Router MikroTik. Anda dapat melihat gambar 1.1, dimana Router MikroTik ditempatkan di antara jaringan lokal (LAN) dan jaringan Internet. Jaringan lokal itu terdiri dari beberapa komputer yang ingin mendapatkan akses Internet. Router MikroTik dapat berperan sebagai penghubungnya, sekaligus mengatur lalu lintas Internet, baik yang masuk maupun keluar dari jaringan lokal tersebut.

Router MikroTik akan mampu menyaring (filter) akses Internet yang bisa diberikan, dan apa saja yang tidak boleh. Jika diinginkan, Router MikroTik akan mampu memblokir web site tertentu, bahkan pemblokiran bisa dilakukan menurut pengaturan waktu. Router MikroTik juga akan mampu membagi bandwidth Internet yang akan digunakan komputer user, sehingga tidak ada user yang merasa lambat mengakses Internet karena adanya user lain yang sedang mendownload file-file berukuran besar.

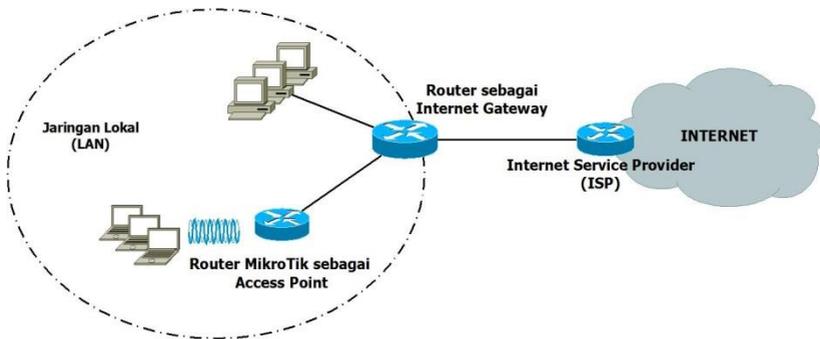
Peran sebagai Internet Gateway inilah yang akan dibahas di buku MikroTik Kung Fu Kitab 1 ini.



Gambar 1.1
Router sebagai Internet Gateway bagi LAN

Sebagai Access Point (Indoor/Outdoor)

Beberapa Router MikroTik dilengkapi dengan interface wireless, sehingga dapat berfungsi sebagai Access Point pada jaringan wireless (Wi-Fi). Anda dapat menggunakannya untuk Hotspot berskala kecil, seperti Hotspot Cafe, Sekolah atau Kantor. Anda juga dapat menggunakannya untuk jaringan yang lebih besar seperti RT/RW Net atau bahkan jaringan sekelas Wireless ISP (WISP). Router MikroTik dengan interface wireless dipasarkan dengan berbagai macam tipe dan dukungan terhadap penggunaan Antena untuk memperluas jangkauan jaringan.

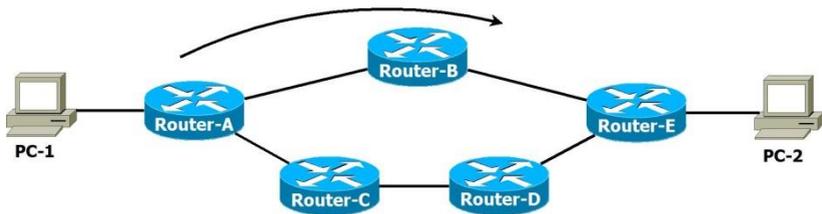


Gambar 1.2
Wireless Router sebagai Access Point

Pada buku ini, akan dibahas bagaimana menggunakan Router MikroTik sebagai perangkat hotspot berskala kecil. Untuk jaringan skala lebih besar akan dibahas pada buku MikroTik Kung Fu seri berikutnya. Dan jika Anda ingin mendalami penggunaan Router MikroTik sebagai Access Point, Anda dapat membaca buku **“Implementasi Wireless Indoor dengan Router MikroTik”**, terbitan Jasakom.

Sebagai Intermediary Device (routing)

Inilah sebenarnya yang merupakan fungsi utama router, menghubungkan beberapa jaringan (network) dan berusaha untuk menentukan jalur terbaik bagi paket data yang ingin menjangkau komputer tujuan. Anda dapat melihat gambar 1.3 yang memperlihatkan jaringan yang terdiri dari beberapa Router MikroTik.



Gambar 1.3
Implementasi Routing

Router MikroTik dapat memilihkan jalur terbaik saat PC-1 ingin mengirimkan data ke PC-2, demikian pula sebaliknya. Misalnya, jika Anda berada di komputer PC-1, maka untuk menuju komputer PC-2, Router A akan memilih jalur melalui Router B. Ini karena jalur melalui Router B akan lebih pendek dari pada melalui Router C. Untuk menjalankan Router MikroTik seperti dalam gambar 1.3, pembahasannya dapat Anda baca pada buku **“Konsep Routing dengan Router MikroTik : 100% Connected”**, terbitan Jasakom.

Router MikroTik masih dapat memiliki peran yang lain dalam jaringan komputer, misalnya bisa menjadi VPN Server, Authentication Server, User Manager, Wireless Bridge dan lain-lain.

Bagaimana mendapatkan Router MikroTik?

Router MikroTik adalah router yang diproduksi oleh Mikrotikls. Mikrotikls merupakan perusahaan pembuat perangkat jaringan yang berkedudukan di Kota Riga, Latvia. Produk utama dari perusahaan ini sebenarnya adalah sistem operasi router yang diberi nama RouterOS. Sistem operasi ini dapat di-install pada komputer biasa (x86) sehingga bisa menjadikan komputer tersebut sebagai router. Mikrotikls juga memproduksi perangkat keras router sendiri yang diberi nama RouterBoard. Sistem operasi yang digunakan di RouterBoard adalah RouterOS.

Selain mampu diinstall pada komputer biasa maupun RouterBoard, RouterOS merupakan sistem operasi router yang bisa diinstall pada hardware lain. Ini mendorong beberapa produsen membuat hardware yang dapat menjalankan RouterOS. Sebagai contoh, vendor **mikrobits.com** juga membuat hardware router yang menggunakan RouterOS sebagai sistem operasinya.

Dengan demikian, jika kita menyebut Router MikroTik, maka bisa saja perangkat tersebut adalah sebuah komputer yang menjalankan RouterOS. Atau, Router MikroTik bisa saja berupa sebuah RouterBoard yang memang merupakan perangkat keras khusus router, yang tentunya juga akan menggunakan RouterOS sebagai sistem operasinya. Atau pun perangkat lain yang juga menggunakan RouterOS sebagai sistem operasinya. *All Powered by MikroTik*, begitu kira-kira bahasa kerennya. Karena apa pun perangkatnya, sistem operasinya tetap adalah RouterOS buatan Mikrotikls.

Dengan demikian, untuk mendapatkan Router MikroTik, Anda dapat menempuhnya dengan beberapa cara, yaitu :

1. Menginstallnya di Personal Computer (PC) biasa.

Bila ini yang ingin dilakukan, Anda harus mendownload file ISO dari RouterOS. Kemudian memburning file tersebut di CD

dan melakukan instalasi pada PC Anda. Anda dapat mendownload file ISO tersebut pada web site www.mikrotik.com/download. Perlu diingat bahwa RouterOS adalah perangkat lunak berlisensi. Artinya Anda harus membayar lisensi untuk menggunakannya. Pada web site mikrotik.com, file ISO yang disediakan merupakan versi trial dari RouterOS. Versi trial ini hanya bisa digunakan selama 24 jam, jika ingin menggunakannya secara terus menerus, Anda harus memasukkan lisensi. Lisensi ini dapat dibeli pada web site www.mikrotik.co.id.

2. Membeli dedicated router.

Cara ini relatif lebih menguntungkan, karena Anda akan membeli perangkat router yang sudah dilengkapi dengan RouterOS. Anda bisa saja memilih produk RouterBoard maupun MikroBits. Tentunya harga akan bervariasi sesuai dengan spesifikasi hardware yang ditawarkan. Jika cara ini yang Anda pilih, maka lisensi tidak menjadi persoalan lagi. Umumnya RouterBoard maupun Mikrobits yang dijual, sudah dilengkapi dengan RouterOS dengan lisensi tertentu (bukan versi trial lagi). Untuk melihat berbagai macam jenis dedicated Router, Anda dapat melihat web site www.mikrotik.co.id.

3. Menggunakan Cloud Host Router

Cloud Host Router (CHR) merupakan versi RouterOS yang ditujukan untuk penggunaan di mesin virtual. Bila Anda ingin menjalankan RouterOS pada mesin virtual seperti VMWare, Hyper-V, VirtualBox, KVM maupun Proxmox VE, maka menggunakan CHR merupakan pilihan yang bijak. Ini karena CHR merupakan versi RouterOS yang tidak membutuhkan lisensi khusus seperti versi RouterOS yang lain.

Jika ingin membeli dedicated router, maka pertimbangan spesifikasi sangatlah penting, karena akan berkaitan dengan dana yang Anda miliki dan network yang akan ditangani. Yang harus diperhatikan

adalah kapasitas CPU dan Memori. Jika network yang ingin ditangani adalah network yang besar dengan lalu lintas data yang padat, maka Anda harus membeli router dengan kapasitas CPU dan Memori yang besar.

Begitu juga jika Anda ingin menjadikan Router MikroTik sebagai Access Point maupun Station dalam jaringan nirkabel. Tentunya Anda harus membeli dedicated router yang memiliki interface wireless.

Instalasi MikroTik RouterOS

Pada sub bab sebelumnya, salah satu cara untuk mendapatkan Router MikroTik adalah membangunnya dengan perangkat Personal Computer (PC) biasa. Dan jika ingin menggunakan RouterOS pada Personal Computer, maka Anda harus melakukan tahapan instalasi RouterOS. Selain itu, yang harus diperhatikan adalah komputer yang akan digunakan harus memiliki minimal 2 (dua) interface jaringan. Karena umumnya motherboard komputer hanya memiliki sebuah interface jaringan onboard, maka Anda harus menambahkan paling tidak sebuah kartu jaringan lagi (LAN Card) untuk membangun Router MikroTik.

Sebagai catatan, bagi Anda yang akan menggunakan RouterBoard, MikroBits maupun CHR, maka sub bab ini tidak perlu Anda baca 😊.

Jika sudah mempersiapkan hardware komputer, maka Anda akan dihadapkan oleh dua pilihan lagi, yaitu :

- Menggunakan Disk on Module
- Melakukan instalasi RouterOS pada hard disk biasa.

Jika ingin menggunakan Disk On Module (DOM), maka Anda tidak perlu repot-repot. Anda tinggal membeli DOM yang didalamnya sudah terinstall sistem operasi MikroTik RouterOS berlisensi dan

langsung memasangnya pada motherboard komputer. Contoh DOM yang dijual dapat dilihat pada alamat www.mikrotik.co.id atau situs toko online lainnya. Contoh DOM terlihat pada gambar berikut :



Gambar 1.4
Disk On Module (DOM) SATA
(sumber : www.mikrotik.co.id)

Sedangkan, jika memilih untuk menginstall RouterOS pada hard disk biasa, maka terlebih dahulu Anda harus mendownload file ISO dari RouterOS. Setelah file ISO berhasil didownload, file tersebut harus di-burn ke dalam sebuah CD. Langkah selanjutnya adalah melakukan instalasi RouterOS yang prosedurnya relatif sama dengan prosedur instalasi sistem operasi pada umumnya. Adapun langkah instalasinya adalah sebagai berikut :

1. Memasukkan CD Instalasi MikroTik RouterOS ke dalam CD/DVD ROM.
2. Memastikan urutan boot pertama PC Anda adalah CD/DVD ROM. Konfigurasi ini dapat dilakukan pada menu BIOS.
3. Setelah itu akan muncul tampilan seperti berikut yang akan menanyakan fitur-fitur apa yang akan disertakan pada router Anda.

```

Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.

[ X ] system          [ ] hotspot          [ ] routing
[ ] ppp              [ ] ipv6              [ ] security
[ ] dhcp             [ ] kvm                [ ] ups
[ ] advanced-tools  [ ] lcd                [ ] user-manager
[ ] calea            [ ] mpls              [ ] wireless@
[ ] dude             [ ] multicast
[ ] gps              [ ] ntp

system (depends on nothing):
Main package with basic services and drivers

```

4. Menekan tombol **a** pada keyboard untuk memilih semua paket instalasi, kemudian menekan tombol **i** untuk melakukan instalasi.
5. Langkah selanjutnya adalah mengikuti perintah-perintah instalasi yang meminta Anda untuk melakukan format hard disk. Setelah itu instalasi akan dimulai seperti pada gambar berikut :

```

Formatting boot partition 100%

installed system-6.42.2
installed wireless@-6.42.2
installed user-manager-6.42.2
installed ups-6.42.2
installed security-6.42.2
installed routing-6.42.2
installed ntp-6.42.2
installed multicast-6.42.2
installed mpls-6.42.2
installed lcd-6.42.2
installed kvm-6.42.2
installed ipv6-6.42.2
installed hotspot-6.42.2
installed gps-6.42.2
installed dude-6.42.2
installed calea-6.42.2
installed advanced-tools-6.42.2
installed dhcp-6.42.2
installed ppp-6.42.2

Software installed.
Press ENTER to reboot

```

6. Setelah itu PC Anda akan direboot, dan sebelum PC tersebut boot kembali, CD instalasi RouterOS harus dikeluarkan dari CD/DVD ROM.
7. Jika PC tersebut sudah boot kembali, maka proses instalasi Router OS telah selesai.
8. Anda dapat login ke dalam Router MikroTik dengan menggunakan username : admin dengan tidak memasukkan password (no password).

Lisensi RouterOS

RouterOS merupakan sistem operasi router berlisensi. Lisensi tersebut dibagi dalam beberapa level, mulai level 0 yang merupakan versi trial (demo) sampai dengan level 6 yang merupakan level tertinggi. Buku ini tidak akan membahas secara detail perbedaan setiap level. Dengan mempelajari konfigurasi-konfigurasi yang ada di buku ini, maka dengan sendirinya Anda akan memahami perbedaan di setiap level. Ada kalanya untuk mempelajari sesuatu kita harus menggunakan alur maju mundur ®. Terkadang kita harus belajar teori dulu baru melakukan praktek, namun di kondisi tertentu kita mudah memahami teori setelah menjalani prakteknya.

Sebagai gambaran, perbedaan setiap level tersebut dapat dilihat pada tabel berikut :

Tabel 1.1

Level dari RouterOS

Sumber : <http://wiki.mikrotik.com/wiki/Manual:License>

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

Khusus untuk Cloud Host Router (CHR), terdapat versi berbayar dan versi gratis (free). Untuk versi gratis, semua fitur RouterOS pada CHR akan dapat digunakan dengan baik. Namun, versi gratis ini akan membatasi trafik yang keluar dan masuk ke dalam Router MikroTik hanya sebesar 1 Mbps. Jika kurang puas dengan batasan 1 Mbps tersebut, mungkin Anda dapat mencoba versi trial dari CHR yang dapat digunakan selama 60 hari. Penggunaan CHR belum akan dibahas pada buku ini. CHR umumnya digunakan untuk skenario-skenario jaringan yang cenderung rumit.

Versi RouterOS

RouterOS juga direlease dalam berbagai versi, versi terakhir tentu memiliki kelebihan dari versi-versi sebelumnya. Dan terkadang menu-menu konfigurasi akan berbeda antar satu versi dengan versi lainnya. Pada saat buku ini ditulis, versi RouterOS yang tersedia adalah RouterOS 6.42.2

Jadi, setelah Anda memiliki Router MikroTik, Anda harus melihat versi berapa RouterOS yang digunakan dan berada di level berapa RouterOS tersebut. Tentu versi yang terkini dengan level yang tertinggi adalah pilihan yang paling baik.

Apa yang harus menjadi Modal Anda

Saya menyempatkan untuk menuliskan sub bab ini, dengan maksud mempermudah Anda dalam memahami buku ini. Karena untuk bisa memahami pembahasan buku ini, Anda dituntut untuk memiliki beberapa kemampuan dasar tentang jaringan komputer. Dengan beberapa pengetahuan dasar tersebut, skenario dan perintah-perintah yang ada di buku ini akan mudah dipahami. Alangkah baiknya Anda sudah memiliki pengetahuan berikut :

- **Dasar jaringan,**

Pengetahuan dasar jaringan ini antara lain, Anda sudah pernah membuat jaringan LAN biasa untuk kepentingan *sharing* folder atau printer. Anda sudah mengerti pengkabelan jaringan maupun IP Address. Untuk IP Address itu sendiri, Anda sebaiknya mengerti penggunaan prefix atau "/". Paling tidak Anda mengerti pada saat skenario jaringan menuliskan 192.168.1.0/24.

- **Layanan Internet,**

Untuk layanan Internet, paling tidak Anda bisa menggunakan layanan browsing ke Internet dengan menggunakan web browser. Mahir menggunakan Download Manager juga

merupakan nilai tambah pada saat Anda akan menguji konfigurasi di Router MikroTik.

- **Pengujian Jaringan,**

Menguji jaringan yang dimaksudkan adalah Anda bisa menggunakan tool “ping” untuk menguji terhubung tidaknya suatu komputer ke jaringan maupun ke Internet.

- **TCP/IP Fundamental,**

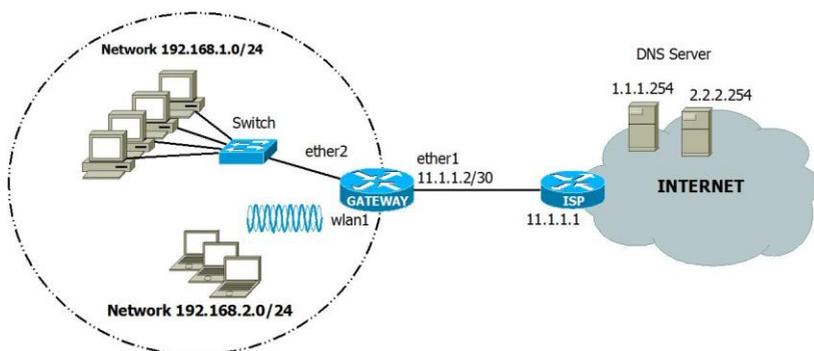
Nah, ini yang sering kita lupakan atau tepatnya malas kita pelajari. Ini memang bisa dimaklumi, karena mempelajari teori tentang TCP/IP sangatlah menguras pikiran. Namun sebenarnya manfaat yang akan Anda dapatkan sangatlah besar pada saat akan terjun di lapangan. Pada pembahasan TCP/IP Fundamental, paling tidak Anda akan mengetahui tujuan penggunaan IP Address (*source address* maupun *destination address*) maupun penggunaan *port number* (*source port* maupun *destination port*). Anda juga sebaiknya mengetahui penggunaan protokol TCP, UDP maupun ICMP.

Uraian di atas adalah modal dasar, namun jangan sampai Anda mundur untuk membaca keseluruhan isi buku ini hanya karena salah satu kemampuan dasar yang tadi disebutkan, tidak Anda miliki. Adakalanya, Anda hanya perlu tahu bahwa ada mobil yang mempunyai setir, gas, rem dan kopling. Masalah bisa tidaknya Anda mengendarai mobil, itu adalah persoalan waktu ☺.

Skenario Jaringan

Skenario jaringan yang digunakan di buku ini dapat dilihat pada gambar 1.5. Pada gambar tersebut Router MikroTik digunakan untuk membagi koneksi Internet dari Internet Service Provider (ISP). Koneksi Internet akan dibagi pada 2 (dua) network, masing-masing network 192.168.1.0/24 (kabel) dan network 192.168.2.0/24 (wireless). Jika melihat skenario tersebut maka dibutuhkan dedicated router yang memiliki interface wireless. Sehingga untuk mempraktekan

keseluruhan isi buku ini, sebaiknya Anda menyiapkan RouterBoard yang memiliki interface wireless.



Gambar 1.5
Skenario yang akan dijalankan

Pada gambar 1.5, juga terlihat interface yang digunakan adalah interface *ether1*, *ether2* dan *wlan1*. Sebagai informasi awal, Router MikroTik akan memberi nama interface ethernet (kabel) dengan nama *ether1*, *ether2*, *ether3* dan seterusnya, sedangkan interface wirelessnya diberi nama *wlan1*, *wlan2* dan seterusnya. Interface-interface tersebut berguna sebagai penghubung Router MikroTik ke jaringan.

Penulisan buku ini menggunakan RouterBoard RB951-2n, yang memiliki 5 buah interface ethernet dan sebuah interface wireless. Adapun versi RouterOS yang digunakan adalah versi 6.42.2 dengan lisensi Level 4. Walaupun nantinya Anda menggunakan versi RouterOS yang berbeda dengan apa yang digunakan di buku ini, maka perintah-perintah konfigurasi yang digunakan akan relatif sama, selama Anda masih menggunakan versi 6.xx.



Gambar 1.6
RB951-2n

Perintah Router MikroTik

Router MikroTik dapat dikonfigurasi secara grafis maupun menggunakan perintah-perintah ala CLI (Command Line Interface). Melakukan konfigurasi Router MikroTik secara grafis dapat Anda lakukan dengan menggunakan aplikasi WinBox maupun melalui web browser. Melakukan konfigurasi secara grafis memang sangat mudah, Anda tinggal melihat menu-menu yang tersedia, memilih menu yang diinginkan, klik sana – klak sini dan konfigurasi Anda selesai.

Namun jika menggunakan CLI untuk melakukan konfigurasi, maka Anda harus mengingat perintah-perintah apa saja yang dapat diberikan. Cara ini relatif lebih sulit, namun banyak literatur Router MikroTik di Internet ditulis dengan menggunakan command line. Itulah sebabnya buku ini menitikberatkan penggunaan command line saat akan melakukan konfigurasi. Sebenarnya, dengan menguasai perintah-perintah Router MikroTik melalui CLI, Anda akan mendapatkan kemudahan jika dikemudian hari akan melakukan konfigurasi dengan prosedur klik-klak mouse ☺.

Agar Anda tidak mengalami kesalahan dalam menggunakan perintah-perintah Router MikroTik, maka penting untuk memahami persepsi penulisan perintah di buku ini.

1. Jika ada uraian seperti berikut :

```
[admin@MikroTik] > ip address add address=11.1.1.2/30 interface=ether1
```

Maka yang Anda ketik hanyalah

```
ip address add address=11.1.1.2/30 interface=ether1
```

2. Selanjutnya jika tertulis seperti berikut :

```
[admin@gateway] > ip firewall nat add chain=srcnat \
src-address=192.168.1.0/24 action=masquerade
```

Tanda “\” menandakan bahwa perintah tersebut bersambung ke baris di bawahnya. Jadi, perintah tersebut sebenarnya adalah

```
ip firewall nat add chain=srcnat src-address=192.168.1.0/24 action=masquerade
```

Mempersiapkan Router MikroTik

Sebelum membaca dan mempraktekan isi dari buku ini, sebaiknya Anda mempersiapkan terlebih dahulu Router MikroTik yang akan digunakan. Persiapan ini meliputi prosedur reset konfigurasi dan mempersiapkan konfigurasi awal sehingga bisa sesuai dengan skenario pada buku ini.

Prosedur Reset

Pada saat Anda membeli RouterBoard yang baru, maka router tersebut sebenarnya sudah memiliki sistem operasi MikroTik RouterOS dengan konfigurasi default. Konfigurasi default ini relatif sudah lengkap sehingga RouterBoard dapat langsung diterapkan pada jaringan. Konfigurasi tersebut sudah memungkinkan beberapa komputer user mengakses Internet melalui RouterBoard. Konfigurasi default ini akan memberikan IP Address 192.168.88.1/24 pada interface *ether2*. Sedangkan username yang bisa Anda gunakan untuk masuk (log in) kedalam Router MikroTik adalah "admin", username ini dapat digunakan tanpa menggunakan password.

Jika RouterBoard Anda bukan merupakan router yang baru atau router yang pernah digunakan orang lain, maka sebaiknya Anda melakukan prosedur reset. Prosedur reset ini akan mengembalikan konfigurasi router Anda menjadi konfigurasi default. Untuk mempelajari buku ini sekaligus mempraktekannya, maka saya menyarankan Anda untuk melakukan prosuder reset terlebih dahulu jika ternyata router Anda sudah pernah dikonfigurasi sebelumnya.

Adapun prosedur reset yang dibahas sub bab ini adalah prosedur reset untuk RouterBoard seri 951. Untuk RouterBoard dengan seri yang lain, mungkin Anda harus melakukan prosedur yang berbeda.

RouterBoard 951-2n memiliki sebuah tombol reset (RES). Tombol reset tersebut berada di sekitar port ethernet dan merupakan tombol kecil yang tersembunyi. Anda membutuhkan pengungkit kecil atau pulpen untuk menekan tombol tersebut. Adapun prosedur melakukan reset dengan menggunakan tombol tersebut adalah sebagai berikut :

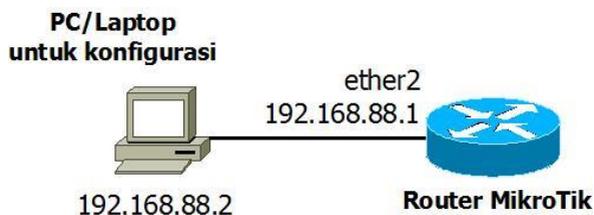
1. Pastikan semua kabel UTP tidak ada terhubung ke port ethernet (port jaringan) dari Router MikroTik.
2. Pastikan juga kabel Adaptor (power) tidak tercolok ke Router MikroTik, sehingga Router MikroTik dalam kondisi off.
3. Setelah semua kabel UTP dan Adaptor tidak terhubung, ambilah pengungkit kecil untuk menekan tombol reset.
4. Sambil menekan tombol reset tersebut, colokkan kembali kabel power dari Adaptor, sehingga Router MikroTik mendapatkan catuan listrik, ini dilakukan dengan tetap menekan tombol reset. Jika tombol reset terlepas, maka prosedur reset harus Anda ulangi dari awal.
5. Sambil menekan tombol reset tersebut, Anda akan melihat lampu (LED) ACT akan berkedip-kedip, tetap pertahankan menekan tombol tersebut sampai LED ACT tersebut padam.
6. Setelah LED ACT padam, Anda harus tetap menekan tombol reset tersebut sampai semua LED indikator dari port ethernet menyala sebentar kemudian padam. Untuk menunggu semua LED indikator dari port ethernet menyala, Anda membutuhkan waktu kira-kira 20 sampai 40 detik.
7. Setelah semua LED indikator pada port ethernet menyala kemudian padam, lepaskanlah kabel power Adaptor sehingga Router MikroTik off kembali.
8. Colokkan kembali kabel power Adaptor untuk menghidupkan Router MikroTik.
9. Router MikroTik Anda sudah dapat digunakan kembali dengan konfigurasi default.

Beberapa seri RouterBoard tidak memiliki tombol reset yang dapat Anda jangkau dari luar. Anda harus membuka casing dari Router

MikroTik tersebut untuk mencari tombol reset yang ada di motherboard dari Router MikroTik tersebut .

Login ke Router MikroTik

Setelah Anda mengembalikan konfigurasi Router MikroTik menjadi konfigurasi default, maka IP Address di *ether2* adalah 192.168.88.1/24. Sehingga untuk login ke Router MikroTik dan melakukan konfigurasi-konfigurasi yang ada di buku ini, Anda harus membuat topologi seperti berikut :



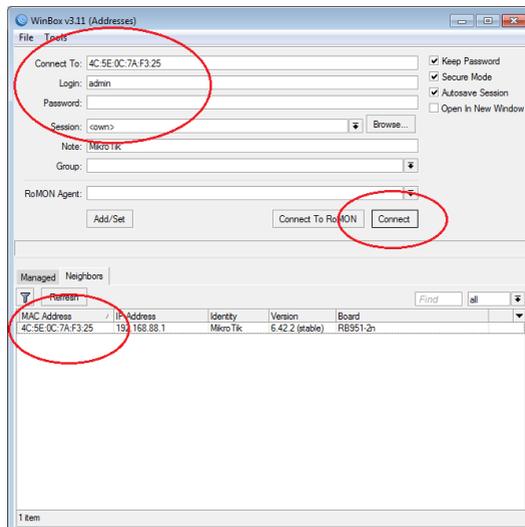
Gambar 1.7
Topologi untuk keperluan konfigurasi

Ada beberapa cara untuk login ke Router MikroTik. Anda dapat menggunakan akses web browser, SSH, Telnet maupun dengan menggunakan aplikasi WinBox. Untuk login ke Router MikroTik dengan menggunakan interface web (web based), Anda tinggal menggunakan browser dengan menyetikkan URL <http://192.168.88.1>. Sedangkan jika Anda ingin menggunakan SSH maupun Telnet, Anda harus memiliki aplikasi SSH Client maupun Telnet Client. Untuk sistem Linux, aplikasi SSH Client/Telnet Client sudah terinstall secara default. Namun untuk komputer dengan sistem Windows, Anda harus menggunakan aplikasi tambahan seperti putty. Putty dapat Anda download di web site berikut <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

Pada buku ini, akses konfigurasi akan dilakukan dengan menggunakan aplikasi WinBox yang menyediakan menu grafis.

Namun konfigurasi akan tetap dilakukan dengan mengetikkan perintah-perintah ala command line pada WinBox. WinBox dapat Anda download pada web site <https://mikrotik.com/download>. Aplikasi ini tidak membutuhkan prosedur instalasi, Anda cukup mendownloadnya dan langsung menjalankannya. Aplikasi WinBox yang digunakan pada buku ini adalah WinBox versi 3.11.

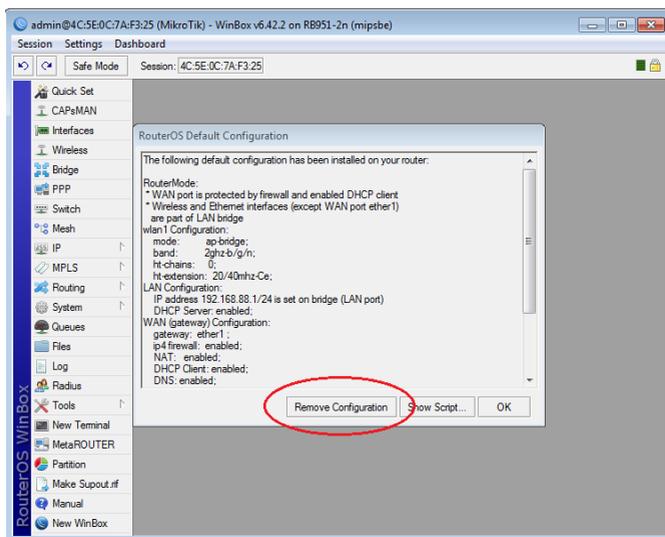
Setelah menjalankan aplikasi WinBox, Anda dapat login ke dalam Router MikroTik dengan menggunakan IP Address. Selain itu, aplikasi WinBox juga memiliki kelebihan yang memungkinkan Anda login ke Router MikroTik hanya dengan menggunakan MAC Address, seperti gambar berikut :



Gambar 1.8
Login ke router dengan MAC Address

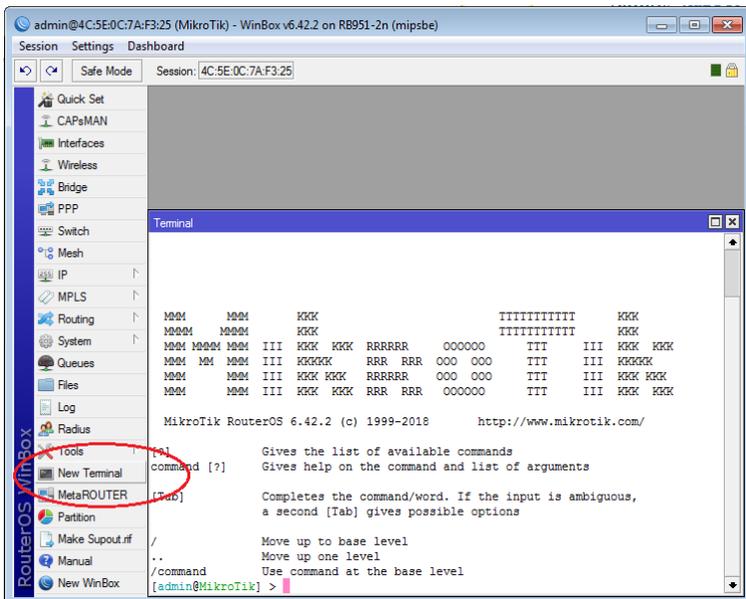
Untuk kemudahan proses login, disarankan untuk menggunakan MAC Address, ini untuk mencegah terjadinya logout dari Router MikroTik manakala Anda menghapus IP Address yang ada pada interface *ether2*. Anda dapat menggunakan Login: admin dengan kolom Password dikosongan

Setelah berhasil login ke Router MikroTik dengan menggunakan aplikasi WinBox, maka Anda akan mendapati kotak dialog yang menanyakan apakah Anda akan menggunakan konfigurasi default dari RouterBoard ataukah ingin melakukan konfigurasi sendiri. Kotak dialog ini akan muncul jika Router MikroTik memiliki konfigurasi default. Konfigurasi default umumnya terdapat pada Router MikroTik yang berada dalam kondisi baru, atau Router MikroTik yang telah mengalami prosedur reset (melalui tombol RES). Untuk kepentingan penulisan buku ini, disarankan untuk tidak menggunakan konfigurasi default. Bukankah Anda ingin mempelajari Router MikroTik dengan buku ini, sehingga konfigurasi default tersebut sebenarnya tidak dibutuhkan 😊. Anda sebaiknya memilih tombol Remove Configuration, seperti gambar berikut.



Gambar 1.9
Remove Configuration

Selanjutnya, akan terlihat menu-menu konfigurasi di sebelah kiri. Menu-menu ini memungkinkan Anda untuk melakukan konfigurasi router dengan cara melakukan klik-klak mouse ☺. Namun, karena pembahasan buku ini akan menggunakan konfigurasi-konfigurasi dalam bentuk command line, maka Anda sebaiknya menggunakan menu **New Terminal** untuk mengetikkan baris-baris konfigurasi Router MikroTik, seperti gambar berikut :



Gambar 1.10
New Terminal

Konfigurasi Bridging

RouterBoard 951-2n merupakan router yang memiliki 5 buah interface ethernet (untuk jaringan kabel) dan 1 buah interface wireless (untuk jaringan nirkabel). Konfigurasi default yang bisa

saja Anda dapatkan adalah interface wireless *wlan1* yang ter-bridge dengan interface *ether2*. Anda jangan terlalu memikirkan apakah yang dimaksud dengan konfigurasi bridge tersebut. Pada pembahasan ini, hanya ingin dipastikan agar tidak ada konfigurasi bridge pada interface-interface router Anda. Tentang bridge itu sendiri akan dibahas mendalam pada buku MikroTik Kung Fu Kitab 2, yang merupakan kelanjutan dari buku ini.

Untuk memastikan tidak ada konfigurasi bridge pada setiap interface router, Anda dapat mengetikkan perintah-perintah berikut pada **New Terminal**.

```
[admin@MikroTik] > interface bridge print
Flags: X - disabled, R - running
 0 R name="bridge-local" mtu=1500 l2mtu=1598 arp=enabled
    mac-address=00:0C:42:FB:1B:BD protocol-mode=rstp
    priority=0x8000 auto-mac=no admin-mac=00:0C:42:FB:1B:BD
    max-message-age=20s forward-delay=15s transmit-hold-count=6
    ageing-time=5m
```

Uraian di atas memperlihatkan bahwa Router MikroTik Anda memiliki interface bridge dengan nama *bridge-local*. Anda dapat menghapus interface bridge tersebut dengan perintah sebagai berikut :

```
[admin@MikroTik] > interface bridge remove 0
```

Angka 0 di atas merujuk ke nomor index baris konfigurasi bridge pada saat Anda memberikan perintah *interface bridge print*.

Jika Router MikroTik tidak lagi memiliki konfigurasi bridge, maka pada saat Anda memberikan perintah *interface bridge print* akan terlihat seperti berikut :

```
[admin@MikroTik] > interface bridge print
Flags: X - disabled, R - running
```

Perintah selanjutnya adalah memastikan tidak ada port yang menjadi anggota dari interface bridge tadi. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@MikroTik] > interface bridge port print  
Flags: X - disabled, I - inactive, D - dynamic  
#   INTERFACE      BRIDGE      PRIORITY PATH-COST HORIZON  
0 I ether2-master-lo bridge-local 0x80      10      none  
1 I wlan1           bridge-local 0x80      10      none
```

Untuk menghapusnya, dapat digunakan perintah sebagai berikut :

```
[admin@MikroTik] > interface bridge port remove 0,1
```

Angka 0,1 menandakan Anda akan menghapus baris konfigurasi port bridge dengan nomor index 0 dan 1. Perhatikanlah kolom # yang menunjukkan nomor indeks dari setiap baris konfigurasi. Setelah menghapusnya, pemeriksaan konfigurasi port pada bridge tersebut seharusnya akan memperlihatkan hasil seperti berikut ini.

```
[admin@MikroTik] > interface bridge port print  
Flags: X - disabled, I - inactive, D - dynamic  
#   INTERFACE      BRIDGE      PRIORITY PATH-COST HORIZON
```

Uraian di atas memperlihatkan tidak adanya lagi konfigurasi bridge pada masing-masing interface.

Setelah semua konfigurasi default dan konfigurasi bridge pada setiap interface sudah dihapus maka Anda dapat lanjut membaca Bab 2 dan seterusnya. Pada Bab 2 nanti, sebaiknya Anda membaca sekaligus mempraktekkannya.

End of Chapter

Bab 02

Konfigurasi Dasar

Pada bab ini akan dibahas konfigurasi-konfigurasi dasar, dengan tujuan agar Router MikroTik dapat membagi koneksi Internet yang didapat dari ISP (Internet Service Provider). Koneksi Internet tersebut akan dibagi (share) ke beberapa komputer user yang ada di jaringan lokal. Dengan mempelajari bab ini, Anda diharapkan sudah dapat membangun warnet sederhana atau jaringan lokal kantor/sekolah yang dapat mengakses Internet.

Persiapan Konfigurasi

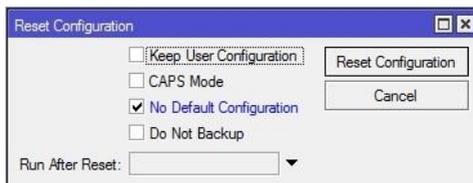
Asumsi yang digunakan pada bab ini adalah Router MikroTik yang tidak memiliki konfigurasi sama sekali. Router MikroTik yang digunakan juga tidak memiliki konfigurasi default yang umumnya terdapat pada Router MikroTik baru.

Jika Anda sudah berhasil login ke dalam Router MikroTik dan belum merasa yakin dengan kondisi router yang akan digunakan,

maka sebaiknya Anda melakukan prosedur reset konfigurasi. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@MikroTik] > system reset-configuration no-defaults=yes  
Dangerous! Reset anyway? [y/N]:  
y
```

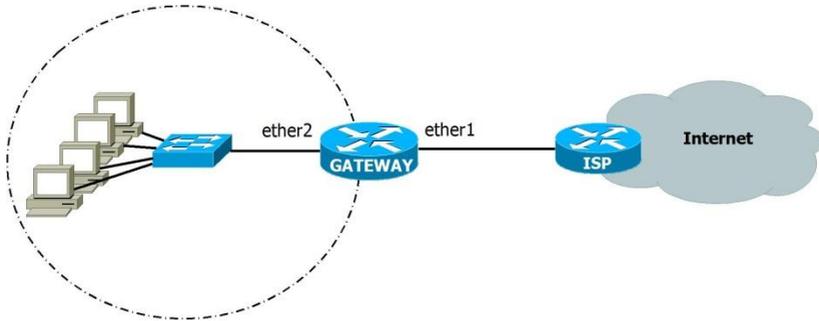
Dengan menggunakan WinBox, menu yang dapat digunakan adalah **System** → **Reset Configuration** → tombol **Reset Configuration**, seperti pada gambar berikut ini.



Gambar 2.1
Reset Configuration

Setelah melakukan prosedur reset, Router MikroTik akan mengalami reboot. Dan setelah proses reboot selesai, maka Router MikroTik tidak lagi akan memiliki konfigurasi dan siap digunakan untuk mempraktekan keseluruhan isi buku ini.

Sebelum melanjutkan ke pembahasan konfigurasi, sebaiknya Anda sudah membangun topologi yang akan digunakan pada bab ini. Topologi tersebut dapat dilihat pada gambar berikut ini.



Gambar 2.2
Topologi Sederhana

Konfigurasi Interface

Sebelum melakukan konfigurasi utama, maka sebaiknya Anda melakukan pemeriksaan interface dari Router MikroTik yang akan digunakan. Ini sebenarnya bertujuan untuk memastikan bahwa interface-interface router dapat diterapkan pada skenario topologi yang digunakan.

Untuk melihat jumlah dan status interface jaringan pada Router MikroTik, Anda dapat menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME      TYPE  ACTUAL-MTU  L2MTU  MAX-L2MTU
0  R  ether1    ether      1500    1600     4076
1  R  ether2    ether      1500    1598     2028
2  ether3    ether      1500    1598     2028
3  ether4    ether      1500    1598     2028
4  ether5    ether      1500    1598     2028
5  X  wlan1     wlan       1500    1600     2290
```

Kolom paling kiri (#) menandakan nomor index, nomor ini berguna sebagai acuan interface mana yang akan dikonfigurasi, misalnya Anda ingin mengkonfigurasi interface *ether1*, maka Anda harus memilih nomor index 0, begitu seterusnya dengan nomor index 1 untuk interface *ether2*.

Simbol R, di depan *ether1* menandakan interface tersebut berada dalam kondisi running (kabel terhubung dengan baik). Jika kabel tidak terhubung dengan baik maka tidak ada label R di depan interface tersebut. Terlihat bahwa hanya *ether1* dan *ether2* yang dihubungkan dengan kabel. Bagaimana dengan *wlan1* yang tidak menggunakan kabel? Interface *wlan1* adalah interface wireless dan akan memiliki label R jika nantinya ada Laptop yang terhubung ke interface tersebut.

Mengganti Nama Interface

Setiap interface memiliki nama, misalnya interface (kabel) ethernet 1 secara default akan memiliki nama *ether1*. Interface (kabel) ethernet 2 akan memiliki nama *ether2* dan seterusnya. Umumnya, interface *ether1* dihubungkan ke Internet (tentunya melalui ISP). Sedangkan interface *ether2* umumnya dihubungkan ke jaringan lokal, tempat dimana komputer-komputer user berada. Sehingga untuk memudahkan konfigurasi, umumnya interface-interface tersebut diberikan nama sesuai fungsinya. Sebagai contoh, perintah berikut ini dapat digunakan untuk mengganti nama dari interface *ether1* dan *ether2*.

```
[admin@MikroTik] > interface set 0 name=ether1-Internet
```

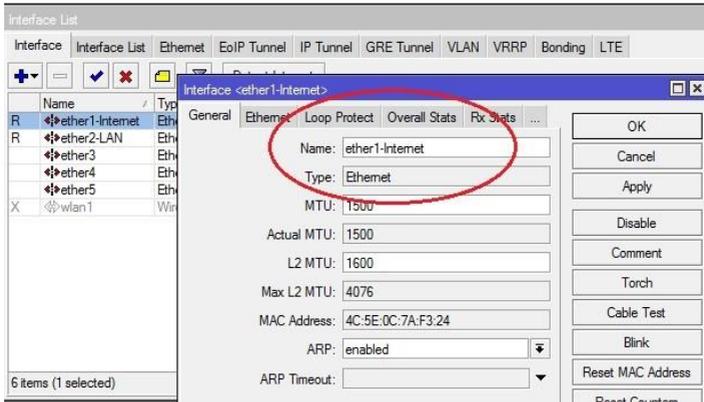
```
[admin@MikroTik] > interface set 1 name=ether2-LAN
```

Setelah itu dapat dilihat kembali apakah interface tersebut sudah memiliki nama yang baru, perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@MikroTik] > interface print
```

```
Flags: D - dynamic, X - disabled, R - running, S - slave
#    NAME                TYPE ACTUAL-MTU L2MTU  MAX-L2MTU
0  R  ether1-Internet      ether    1500  1600    4076
1  R  ether2-LAN          ether    1500  1598    2028
2    ether3              ether    1500  1598    2028
3    ether4              ether    1500  1598    2028
4    ether5              ether    1500  1598    2028
5  X  wlan1               wlan     1500  1600    2290
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Interfaces** → tab **Interfaces**, untuk kemudian melakukan klik 2x interface yang diinginkan. Pada tab **General**, Anda bisa melakukan penggantian pada bagian **Name**, seperti pada gambar berikut ini.



Gambar 2.3
Mengganti Nama Interface

Anda dapat saja mengganti nama interface sesuai keinginan, konfigurasi di atas hanyalah untuk contoh penggunaan nama. Untuk kepentingan efisiensi penulisan buku ini, interface *ether1-Internet* pada contoh di atas, akan tetap dituliskan sebagai interface *ether1*, sedangkan interface *ether2-LAN* akan tetap dituliskan sebagai interface *ether2*.

Menonaktifkan Interface

Jika di depan baris konfigurasi interface terdapat simbol X, maka itu menandakan interface tersebut tidak aktif (disable), atau tidak dapat digunakan. Pada contoh berikut, interface *wlan1* dalam posisi non aktif.

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#      NAME      TYPE  ACTUAL-MTU L2MTU  MAX-L2MTU
0  R  ether1  ether      1500  1600      4076
1  R  ether2  ether      1500  1598      2028
2      ether3  ether      1500  1598      2028
3      ether4  ether      1500  1598      2028
4      ether5  ether      1500  1598      2028
5  X  wlan1   wlan       1500  1600      2290
```

Dengan alasan keamanan, non-aktifkanlah (disable) jika ada interface router yang memang tidak digunakan. Untuk men-disable sebuah interface, misalnya interface *ether3*, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@MikroTik] > interface disable 2
```

Anda dapat melihat kembali status dari interface Router MikroTik dengan perintah berikut :

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#      NAME      TYPE  ACTUAL-MTU L2MTU  MAX-L2MTU
0  R  ether1  ether      1500  1600      4076
1  R  ether2  ether      1500  1598      2028
2  X  ether3  ether      1500  1598      2028
3      ether4  ether      1500  1598      2028
4      ether5  ether      1500  1598      2028
5  X  wlan1   wlan       1500  1600      2290
```

Jika ternyata ingin men-disable beberapa interface sekaligus, misalnya ingin men-disable *ether4* dan *ether5*, maka Anda dapat menggunakan perintah sebagai berikut :

```
[admin@MikroTik] > interface disable 3,4
```

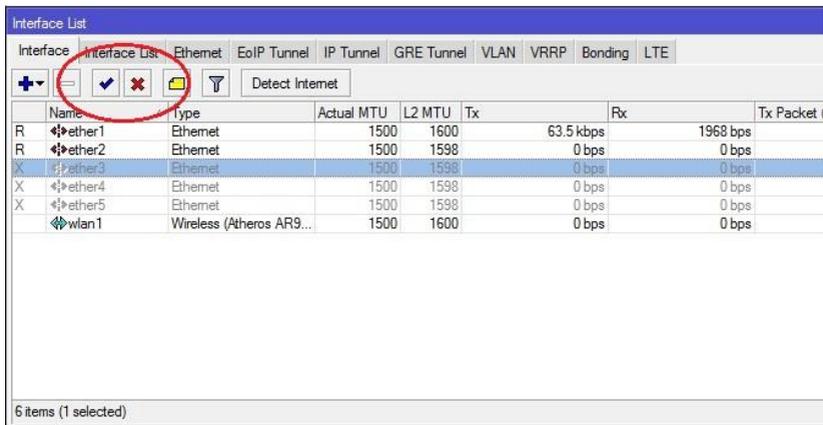
Pada skenario buku ini, Anda nantinya akan menggunakan *wlan1* sebagai interface jaringan wireless (nirkabel), maka untuk mengaktifkan (enable) interface tersebut, perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@MikroTik] > interface enable 5
```

Sehingga konfigurasi interface yang sebaiknya digunakan adalah sebagai berikut :

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME      TYPE  ACTUAL-MTU  L2MTU  MAX-L2MTU
0  R  ether1    ether      1500    1600      4076
1  R  ether2    ether      1500    1598      2028
2  X  ether3    ether      1500    1598      2028
3  X  ether4    ether      1500    1598      2028
4  X  ether5    ether      1500    1598      2028
5  wlan1     wlan      1500    1600      2290
```

Bila menggunakan WinBox, maka konfigurasi dapat dilakukan melalui menu **Interfaces** → tab **Interfaces**. Untuk melakukan disable dan enable interface, Anda tinggal memilih interface yang diinginkan, untuk kemudian melakukan klik pada tombol **Enable** maupun **Disable**, seperti terlihat pada gambar berikut ini.



Gambar 2.4
Menu Interfaces

Konfigurasi Internet Gateway

Tujuan utama dari buku ini adalah menggunakan Router MikroTik sebagai Internet Gateway. Internet Gateway itu sendiri adalah perangkat yang berfungsi memberikan akses Internet kepada beberapa komputer user. Untuk menjalankan fungsi tersebut, harus dilakukan beberapa konfigurasi mendasar pada Router MikroTik yang terdiri dari :

- Konfigurasi IP Address pada setiap interface
- Konfigurasi Default Route atau Default Gateway
- Konfigurasi DNS Server
- Konfigurasi Firewall NAT (masquerade)

Dengan hanya bermodalkan keempat konfigurasi sederhana di atas, komputer-komputer user yang ada di jaringan lokal akan bisa mengakses Internet. Tentunya akses Internet yang diberikan belum mengalami pengaturan atau manajemen yang detail.

Sebelum melakukan konfigurasi-konfigurasi tersebut, perlu diketahui topologi dari jaringan yang akan dibangun, beserta daftar IP Address yang akan digunakan. Konfigurasi tidak dapat dilakukan jika tidak terdapat data yang lengkap tentang topologi maupun IP Address yang akan digunakan.

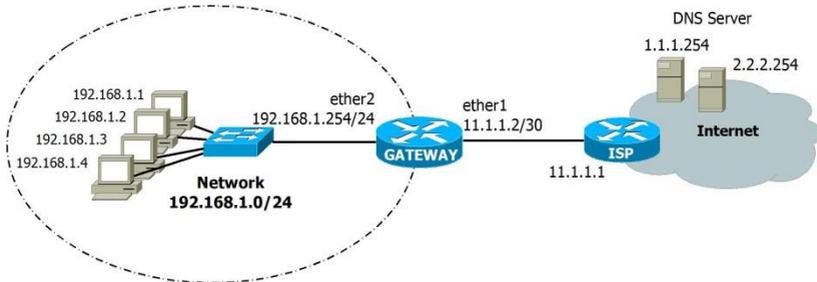
Topologi

Sebelum melakukan konfigurasi, sebaiknya dipersiapkan terlebih dahulu topologi yang akan digunakan. Ini karena konfigurasi selalu dilakukan berdasarkan topologi jaringan. Dari topologi tersebut harus diketahui beberapa hal penting, seperti pada uraian berikut ini.

- IP Address yang diberikan oleh pihak ISP kepada Anda.
- IP Address dari router milik ISP.

- DNS Server yang diberikan oleh ISP (atau DNS Server lain yang bisa digunakan).

Adapun topologi yang akan digunakan pada sub bab ini dapat dilihat pada gambar berikut ini.



Gambar 2.5
Topologi Sederhana

Dari gambar 2.5, terlihat bahwa IP Address yang diberikan oleh ISP kepada Anda adalah 11.1.1.2/30. IP Address ini harus dikonfigurasi pada interface *ether1* yang terhubung ke ISP. Adapun IP Address yang digunakan oleh router ISP adalah 11.1.1.1. Sedangkan DNS Server yang diberikan oleh ISP adalah 1.1.1.254 dan 2.2.2.254. Yang perlu diingat bahwa sesuaikanlah penggunaan DNS Server dengan apa yang diberikan oleh pihak ISP, berapa IP Address dan DNS Server yang bisa digunakan di jaringan mereka. Sebagai pilihan lain., Anda bisa saja menggunakan layanan DNS Server Internet Sehat yang dapat dilihat pada alamat web site <http://dnsbersih.id>.

Dari gambar 2.5 juga terlihat bahwa pada interface *ether2* yang terhubung ke jaringan lokal akan dikonfigurasi IP Address 192.168.1.254/24. IP Address ini bisa saja digantikan dengan IP Address lain, selama IP Address tersebut masih termasuk dalam kategori IP Address Private.

Dalam skenario ini, IP Address pada interface *ether2* adalah 192.168.1.254/24, maka IP Address yang dapat digunakan komputer user adalah IP Address 192.168.1.1 s/d 192.168.1.253.

Konfigurasi IP Address

Berdasarkan skenario topologi yang direncanakan maka IP Address yang akan dikonfigurasi di *ether1* adalah 11.1.1.2/30, perintah yang dapat Anda gunakan untuk mengkonfigurasi IP Address pada *ether1* adalah sebagai berikut :

```
[admin@MikroTik] > ip address add address=11.1.1.2/30 \
interface=ether1
```

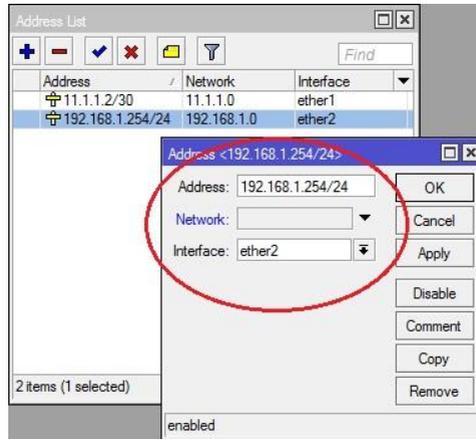
Sedangkan untuk *ether2*, Anda harus mengkonfigurasi IP Address 192.168.1.254/24. Perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@MikroTik] > ip address add address=192.168.1.254/24 \
interface=ether2
```

Setelah kedua IP Address dikonfigurasi, periksalah kembali konfigurasi tersebut dengan perintah sebagai berikut :

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 11.1.1.2/30 11.1.1.0 ether1
1 192.168.1.254/24 192.168.1.0 ether2
```

Bila menggunakan WinBox, maka konfigurasi dapat dilakukan melalui menu **IP → Addresses → tombol Add**, seperti gambar berikut :



Gambar 2.6
Menu IP Address

Jika suatu saat terjadi kesalahan pengisian IP Address, maka untuk menghapus sebuah IP Address, misalnya ingin menghapus IP Address 11.1.1.2 pada *ether1*, Anda dapat menggunakan perintah sebagai berikut :

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 11.1.1.2/30 11.1.1.0 ether1
1 192.168.1.254/24 192.168.1.0 ether2
```

```
[admin@MikroTik] > ip address remove 0
```

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 192.168.1.254/24 192.168.1.0 ether2
```

Oh iya, sebelum melanjutkan membaca dan mempraktekkan buku ini, mohon tambahkan kembali IP Address yang yang sudah Anda remove tadi. Maaf, sudah membuat Anda melakukan pekerjaan tambahan ☺.

Konfigurasi Default Route

Setelah mengkonfigurasi IP Address pada masing-masing interface maka selanjutnya Anda harus mengkonfigurasi default route atau default gateway. Yang akan menjadi default route adalah Router ISP yang berfungsi sebagai gerbang bagi Router MikroTik Anda untuk menuju Internet. Pada skenario ini, Router ISP memiliki IP Address 11.1.1.1.

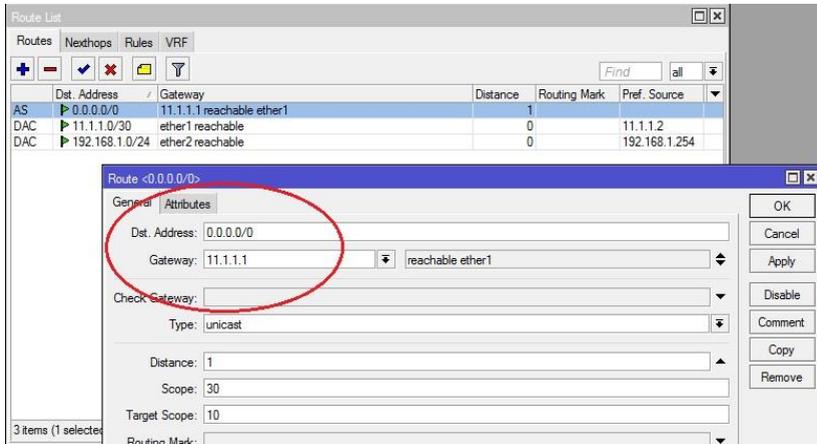
Perintah yang dapat digunakan untuk mengkonfigurasi default route adalah sebagai berikut :

```
[admin@MikroTik] > ip route add gateway=11.1.1.1
```

Periksalah apakah konfigurasi default gateway sudah ada pada tabel routing Router MikroTik. Anda seharusnya mendapati baris dengan *dst-address=0.0.0.0/0* dan *gateway=11.1.1.1*. Perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 A S  0.0.0.0/0          11.1.1.1      1
1 ADC 11.1.1.0/30        11.1.1.2      ether1        0
2 ADC 192.168.1.0/24     192.168.1.254 ether2         0
```

Bila Anda menggunakan WinBox, konfigurasi dapat dilakukan melalui menu **IP → Routes**, tab **Routes** → tombol **Add**.



Gambar 2.7
Konfigurasi default gateway

Konfigurasi DNS Server

DNS Server berfungsi memetakan hostname atau domain web site di Internet menjadi IP Address. Perlu di ingat, bahwa jaringan komputer (termasuk Internet) akan berkomunikasi dengan IP Address bukan dengan nama-nama domain .com, .net, .org dan sebagainya. Itulah mengapa saat melakukan konfigurasi IP Address pada komputer user maupun router yang ingin mengakses Internet, Anda harus melakukan konfigurasi DNS (Domain Name System).

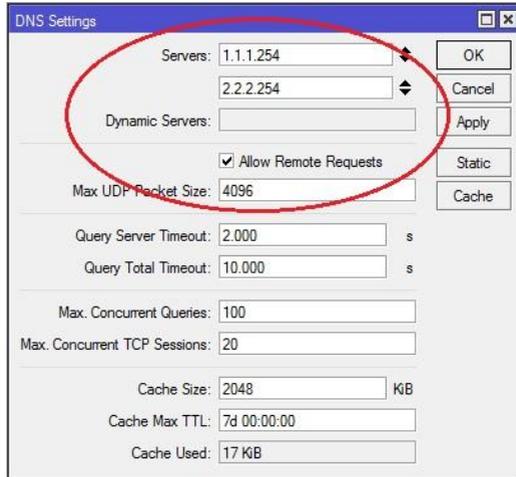
Berdasarkan skenario, yang digunakan adalah DNS Server dengan IP Address 1.1.1.254 dan 2.2.2.254, sehingga perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@MikroTik] > ip dns set servers=1.1.1.254,2.2.2.254 \
allow-remote-requests=yes
```

```
[admin@MikroTik] > ip dns print
      servers: 1.1.1.254,2.2.2.254
dynamic-servers:
allow-remote-requests: yes
max-udp-packet-size: 4096
query-server-timeout: 2s
query-total-timeout: 10s
max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
      cache-size: 2048KiB
cache-max-ttl: 1w
      cache-used: 17KiB
```

Sebagai catatan, parameter *allow-remote-requests=yes*, akan menjadikan Router MikroTik Anda sebagai DNS Server juga. Sehingga nantinya konfigurasi DNS pada komputer user cukup diarahkan ke Router MikroTik, dan tidak lagi di arahkan ke DNS Server milik ISP. Teknik ini dapat menghemat bandwidth karena pertanyaan-pertanyaan DNS hanya akan diberikan ke Router MikroTik Anda.

Bila menggunakan WinBox, maka konfigurasi dapat Anda lakukan melalui menu **IP → DNS**, seperti gambar berikut :



Gambar 2.8
Konfigurasi DNS

Setelah DNS dikonfigurasi, maka seharusnya Router MikroTik sudah terhubung ke Internet. Anda dapat mengujinya dengan menggunakan tool ping pada menu **New Terminal**, seperti berikut ini.

```
[admin@MikroTik] > ping www.google.com
216.239.61.104 64 byte ping: ttl=55 time=162 ms
216.239.61.104 64 byte ping: ttl=56 time=164 ms
216.239.61.104 64 byte ping: ttl=56 time=169 ms
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 162/165.0/169 ms
```

Gunakan CTRL + C untuk menghentikan ping Anda.

Sekali lagi, sebagai catatan konfigurasi DNS, tentunya setiap ISP memiliki DNS Server sendiri. Nantinya, pada penerapan di lapangan, Anda harus menanyakan DNS Server yang diberikan oleh pihak ISP. Intinya, Anda harus menggunakan DNS Server yang akan digunakan sesuai yang disediakan oleh pihak provider.

Bila sampai pada tahapan ini, Router MikroTik Anda belum terhubung ke Internet, maka Anda dapat melakukan pemeriksaan kembali baik itu topologi jaringan yang digunakan, pengkabelan, konfigurasi IP Address di interface router, konfigurasi default route dan tentunya konfigurasi DNS Server.

Masquerade

Router MikroTik pada skenario ini merupakan router yang berada di antara jaringan publik (Internet) dan jaringan lokal (LAN). Router yang berada pada posisi tersebut harus menjalankan Network Address Translation (NAT) yang berfungsi menyembunyikan IP Address pada setiap paket data yang keluar dari komputer user (IP Address Private) menjadi IP Address publik yang ada di *ether1*. Buku ini tidak akan membahas teori tentang NAT secara mendalam, karena saya menginginkan bahwa buku ini merupakan buku terapan praktis.

Saat menerapkan NAT, dikenal teknik masquerade yang merupakan teknik penggantian otomatis IP Address private komputer user menjadi IP Address publik yang ada di Router MikroTik.

Untuk menerapkan konfigurasi NAT dengan teknik masquerade perintah yang dapat digunakan adalah sebagai berikut :

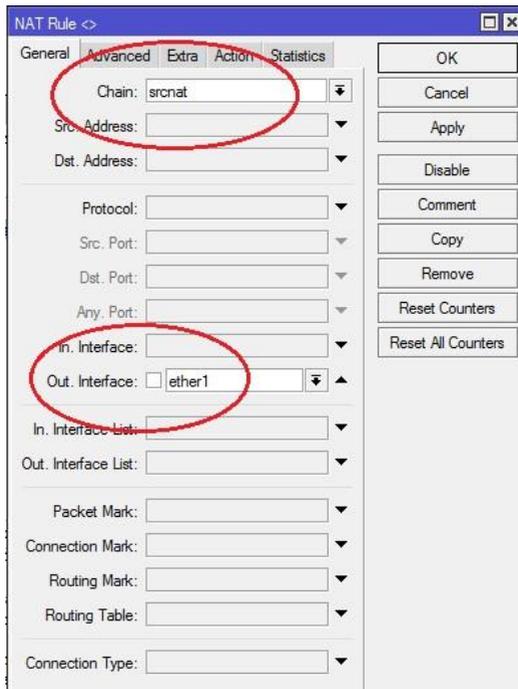
```
[admin@MikroTik] > ip firewall nat add chain=srcnat \
out-interface=ether1 action=masquerade

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

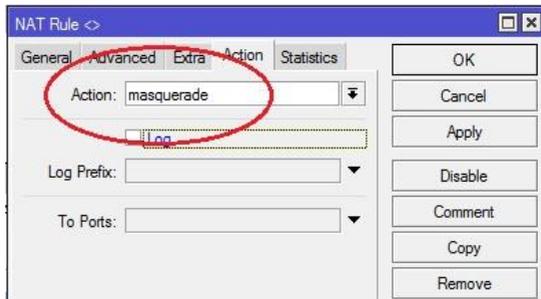
Yang perlu diperhatikan pada perintah di atas adalah parameter *out-interface=ether1*, ini karena interface yang digunakan untuk menuju Internet adalah *ether1*. Begitu juga dengan pilihan *action=masquerade*

yang akan membuat IP Address pengirim (192.168.1.1, 192.168.1.2 dst) yang ada di jaringan lokal akan dikenal di Internet sebagai Router MikroTik dengan IP Address 11.1.1.2.

Bila ingin menggunakan WinBox untuk mengkonfigurasi NAT, maka dilakukan melalui menu **IP** → **Firewall** → tab **NAT**, tombol **Add** → tab **General**, dengan parameter *masquerade* dapat Anda konfigurasi pada tab **Action**.



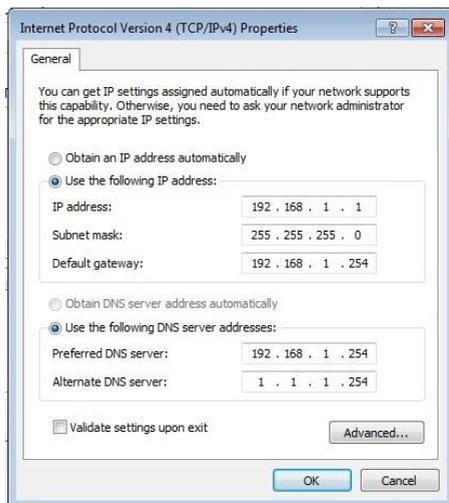
Gambar 2.9
Konfigurasi NAT dengan Masquerade



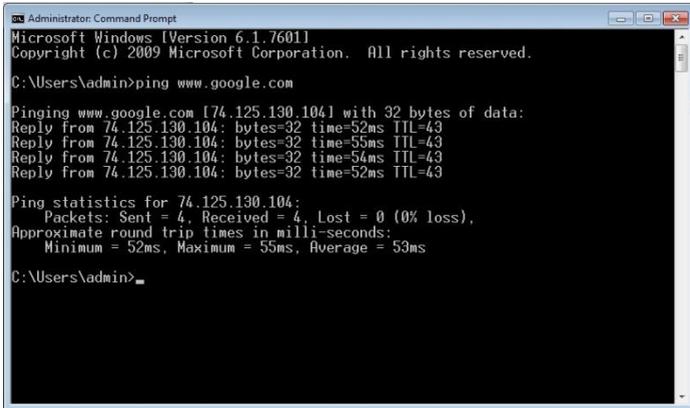
Gambar 2.10
Pilihan masquerade pada tab Action

Setelah Anda mengkonfigurasi NAT dengan masquerade maka seharusnya komputer user sudah dapat mengakses Internet. Anda dapat menguji koneksi Internet dari komputer user. Untuk skenario ini, Anda dapat menggunakan IP Address 192.168.1.1 dengan subnetmask 255.255.255.0 pada komputer user. Jangan dilupakan untuk mengkonfigurasi default gateway ke 192.168.1.254 pada setiap komputer user, begitu juga dengan DNS Server yang dapat dikonfigurasi ke 1.1.1.254 dan 2.2.2.254 atau 192.168.1.254 seperti gambar berikut :

Gambar 2.11
Konfigurasi IP Address pada komputer user



Setelah konfigurasi IP Address pada komputer user berhasil, Anda dapat melakukan pengujian koneksi Internet melalui Command Prompt untuk komputer Windows. Anda dapat melakukan ping ke situs Internet, misalnya www.google.com ataupun langsung mengujinya dengan menggunakan browser Anda, seperti pada gambar berikut ini.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping www.google.com

Pinging www.google.com [74.125.130.104] with 32 bytes of data:
Reply from 74.125.130.104: bytes=32 time=52ms TTL=43
Reply from 74.125.130.104: bytes=32 time=55ms TTL=43
Reply from 74.125.130.104: bytes=32 time=54ms TTL=43
Reply from 74.125.130.104: bytes=32 time=52ms TTL=43

Ping statistics for 74.125.130.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 55ms, Average = 53ms

C:\Users\admin>
```

Gambar 2.12
Pengujian dari Command Prompt komputer user

Sampai pada tahapan ini, saya dapat mengucapkan “Selamat !!! Anda sudah dapat membangun jaringan warnet”. Bukankah semua komputer user Anda sudah dapat ber-Internet? Untuk apa lagi membaca keseluruhan buku ini ☺? Untuk sebuah jaringan dengan biaya konfigurasi 2 M (Makasi Mas!!!), konfigurasi yang dibahas tadi sudahlah cukup ☺.

Meskipun jaringan Anda sudah terhubung ke Internet, tulisan-tulisan pada bab-bab selanjutnya adalah konfigurasi-konfigurasi tambahan yang akan membuat jaringan Anda lebih mudah diatur, lebih aman, mudah dikendalikan dan akan efisien menggunakan bandwidth Internet yang didapatkan dari pihak ISP.

Konfigurasi Tambahan

Konfigurasi pada sub bab Internet Gateway sebelumnya sudah mampu membuat user mengakses Internet. Fungsi Internet Gateway sudah berhasil dijalankan dengan menggunakan beberapa konfigurasi dasar pada sub bab tersebut. Namun, ada beberapa konfigurasi tambahan yang perlu dilakukan untuk mempermudah penggunaan Router MikroTik. Pada sub bab ini akan dibahas beberapa konfigurasi tambahan yang tidak kalah pentingnya.

Konfigurasi User

User yang dimaksud pada pembahasan ini adalah username yang digunakan untuk mengkonfigurasi Router MikroTik Anda. Secara default Router MikroTik akan menggunakan *admin* sebagai username dan tanpa password (null password).

Secara default pula, user yang dapat login ke Router MikroTik dapat dikelompokkan menjadi 3 (tiga) kategori akses, yaitu :

- **Full**, user yang memiliki akses ini merupakan user dengan pangkat tertinggi, user dengan akses Full dapat melakukan konfigurasi-konfigurasi seperti menghapus konfigurasi, menambahkan konfigurasi sampai dengan menambahkan user baru ke dalam sistem MikroTik.
- **Write**, user ini memiliki akses konfigurasi seperti pada user yang memiliki akses Full, namun user di level ini tidak dapat menambahkan user baru. Juga tidak dapat melakukan proses backup konfigurasi
- **Read**, user dengan akses ini hanya mampu melakukan monitoring pada sistem, tidak mampu melakukan konfigurasi-konfigurasi seperti pada user dengan level Write maupun Full.

Untuk melihat daftar user dalam sistem MikroTik, dapat digunakan perintah sebagai berikut :

```
[admin@MikroTik] > user print detail
Flags: X - disabled
 0   ;;; system default user
      name="admin" group=full address="" last-logged-
      in=aug/14/2017 06:34:52
```

Dari uraian di atas, Anda dapat melihat hanya terdapat user *admin* dengan akses Full, sedangkan keterangan *address=""* menunjukkan bahwa user *admin* dapat mengakses (login) Router MikroTik dari mana saja, baik dari dalam jaringan internal (LAN) maupun dari Internet.

Karena secara default user *admin* tidak memiliki password, maka untuk memberikan password *123456* pada user *admin*, Anda dapat menggunakan perintah sebagai berikut :

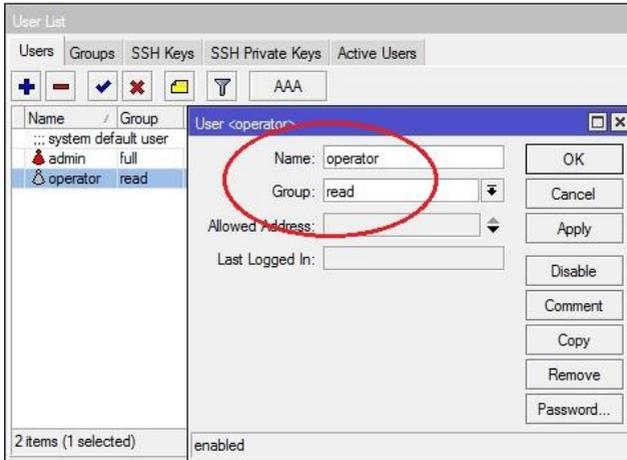
```
[admin@MikroTik] > user set admin password=123456
```

Untuk menambahkan user baru (misalnya user *operator* dengan password *qwerty*) yang hanya memiliki akses Read maka Anda dapat menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > user add name=operator group=read \
password=qwerty

[admin@MikroTik] > user print detail
Flags: X - disabled
 0   ;;; system default user
      name="admin" group=full address="" last-logged-
      in=may/19/2018 08:26:44
 1   name="operator" group=read address=""
```

Bila menggunakan WinBox, maka konfigurasi dapat Anda lakukan melalui menu **System** → **Users** → tab **Users** → tombol **Add**, seperti gambar berikut.



Gambar 2.13
Konfigurasi user pada Mikrotik

Identity

Setiap router harus memiliki identitas atau hostname, sangat berguna agar Anda dapat membedakan router yang satu dengan lainnya, apalagi jika Anda memiliki beberapa router dalam suatu jaringan. Secara default identity yang digunakan adalah *MikroTik*. Untuk mengkonfigurasi identity yang baru, maka perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@MikroTik] > system identity set name=GATEWAY
```

```
[admin@GATEWAY] >
```

Bila menggunakan WinBox, Anda dapat melakukannya melalui menu **System → Identity**



Gambar 2.14
Konfigurasi Identity

NTP (Network Time Protocol) Client

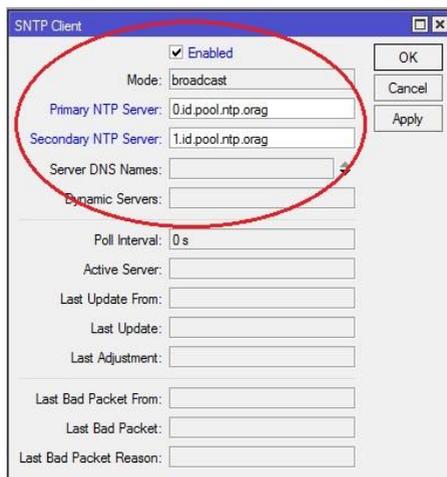
Pada implementasi di lapangan, Router MikroTik sering bekerja berdasarkan waktu dan hari. Karena umumnya tidak memiliki baterai, maka harus dipastikan agar Router MikroTik selalui mengetahui waktu sesuai kondisi yang sebenarnya. Dengan kata lain, parameter waktu pada Router MikroTik harus sinkron dengan kondisi di lapangan.

Untuk melakukan sinkronisasi tersebut, Router MikroTik harus terhubung ke Internet dan melakukan sinkronisasi dengan server NTP yang ada di Internet. Daftar NTP Server untuk wilayah Indonesia adalah sebagai berikut.

- 0.id.pool.ntp.org
- 1.id.pool.ntp.org
- 2.id.pool.ntp.org
- 3.id.pool.ntp.org

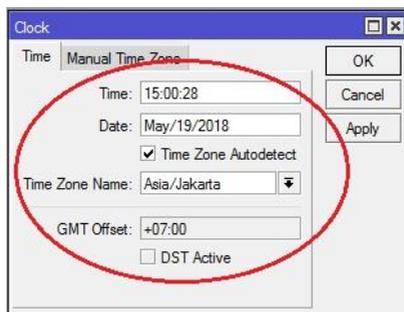
NTP Server lengkapnya dapat dilihat pada alamat <http://www.pool.ntp.org/zone/id>

Untuk melakukan konfigurasi NTP Server, menu yang dapat digunakan adalah **System** → **SNTP Client**, seperti pada gambar berikut ini.



Gambar 2.15
Konfigurasi NTP Client

Selanjutnya, harus dilakukan penyesuaian zona waktu. Jika diambil zona Waktu Indonesia Barat (Jakarta), maka menu yang dapat digunakan adalah **System** → **Clock** → tab **Time**, seperti pada gambar berikut ini.



Gambar 2.16
Konfigurasi Zona Waktu

Jika konfigurasi zona waktu sudah selesai, maka seharusnya waktu pada Router MikroTik akan sinkron dengan waktu yang sebenarnya. Untuk melihatnya dapat digunakan perintah berikut ini.

```
[admin@GATEWAY] > system clock print
      time: 15:04:29
      date: may/19/2018
time-zone-autodetect: yes
      time-zone-name: Asia/Jakarta
      gmt-offset: +07:00
      dst-active: no
```

Dengan menggunakan WinBox, hari, tanggal dan jam juga akan terlihat pada menu **System** → **Clock** → tab **Time**, seperti pada gambar 2.16.

End of Chapter

Bab 03

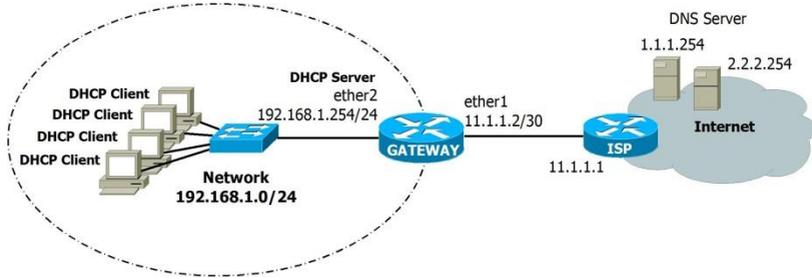
Dynamic Host Configuration Protocol (DHCP Server)

Dynamic Host Configuration Protocol adalah protokol jaringan yang memungkinkan sebuah perangkat jaringan membagi konfigurasi IP Address kepada komputer-komputer user yang membutuhkan. Konfigurasi IP Address ini meliputi IP Address itu sendiri, subnetmask, default gateway dan DNS Server yang dibutuhkan untuk mengakses Internet. Perangkat yang akan membagi konfigurasi IP Address disebut DHCP Server. Anda dapat membangun DHCP Server dengan menggunakan Router MikroTik. Sedangkan komputer yang akan meminta IP Address pada DHCP Server disebut DHCP Client.

DHCP ini diimplementasikan agar Anda tidak perlu repot-repot lagi mengkonfigurasi IP Address pada setiap komputer user, seperti yang dilakukan pada Bab 2 sebelumnya. DHCP banyak diimplementasikan pada hotspot, baik private maupun hotspot untuk publik. Bisa dibayangkan bagaimana sibuknya Anda jika harus memberitahukan IP Address setiap kali ada orang yang ingin menggunakan hotspot Anda. Ditambah lagi pengguna yang datang adalah orang awam yang sama sekali tidak mengetahui bagaimana IP Address itu.

Konfigurasi Dasar

Skenario yang digunakan adalah skenario yang sama dengan topologi yang ada pada Bab 2 sebelumnya, seperti terlihat pada gambar berikut ini.



Gambar 3.1
DHCP Server pada ether2

Pada gambar 3.1, Anda memiliki beberapa komputer user yang membutuhkan IP Address. Komputer user yang membutuhkan IP Address terhubung ke interface *ether2* dari Router MikroTik. Sehingga bila Anda ingin mengaktifkan DHCP Server, maka DHCP Server harus diaktifkan di interface *ether2*.

Selain itu Anda harus memahami parameter apa saja yang harus dikonfigurasi pada DHCP Server. Parameter-parameter tersebut dapat dijabarkan sebagai berikut :

- **Network Address**, parameter ini merupakan network address beserta prefix (subnetmask) yang harus diberikan pada komputer user, dalam skenario ini network addressnya adalah 192.168.1.0/24
- **Gateway**, tentunya komputer user harus memiliki gateway yang akan digunakan mengakses Internet, dalam skenario ini gateway yang harus digunakan komputer user adalah IP Address *ether2* dari Router MikroTik (192.168.1.254).
- **IP Address Pool**, parameter ini akan menentukan berapa jumlah IP Address yang akan Anda berikan kepada sejumlah komputer

user, dalam skenario ini jumlah IP Address yang akan diberikan adalah 192.168.1.1 sampai dengan 192.168.1.10. Anda dapat menyesuaikan dengan jaringan yang akan dibangun.

- **DNS Server**, tentunya komputer user yang akan mengakses Internet membutuhkan DNS Server, dalam skenario ini yang menjadi DNS Server adalah Router MikroTik (192.168.1.254) dan DNS Server milik ISP (1.1.1.254).
- **Lease Time**, DHCP Server bekerja dengan prinsip pinjam-meminjam IP Address. Komputer user akan meminjam konfigurasi IP Address pada DHCP Server. Dalam proses pinjam-meminjam ini, DHCP Server akan memberikan jangka waktu peminjaman IP Address yang ditentukan oleh parameter Lease Time. Selama Lease Time dari sebuah IP Address belum habis, maka IP Address tersebut tidak akan dipinjamkan DHCP Server kepada komputer lain, sekalipun komputer user yang meminjam pertama kali tidak lagi menggunakan IP Address tersebut. Jangan mengkonfigurasikan Lease Time terlalu panjang jika pengguna jaringan Anda sangat dinamis (datang silih berganti), misalnya jika komputer pengguna hanya menggunakan jaringan selama kurang lebih 2 jam. Dalam skenario ini Lease Time akan dikonfigurasikan selama 30 menit.

Untuk mengkonfigurasikan DHCP Server pada interface *ether2* Router MikroTik, Anda dapat melakukannya melalui Wizard yang sudah disediakan. Perintah pertama yang perlu Anda gunakan hanyalah *ip dhcp-server setup* seperti di bawah ini.

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

dhcp server interface: ether2
Select network for DHCP addresses

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

gateway for dhcp network: 192.168.1.254
Select pool of ip addresses given out by DHCP server
```

```
addresses to give out: 192.168.1.1-192.168.1.10
Select DNS servers
```

```
dns servers: 192.168.1.254,1.1.1.254
Select lease time
```

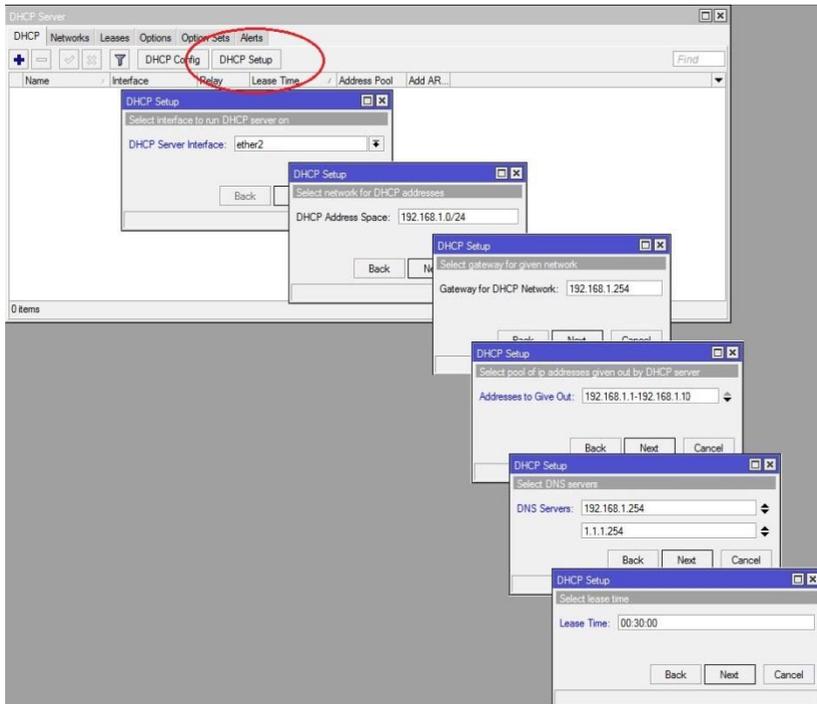
```
lease time: 30m
```

Hasil konfigurasi DHCP Server dapat Anda lihat dengan menggunakan perintah berikut :

```
[admin@GATEWAY] > ip dhcp-server print detail
Flags: D - dynamic, X - disabled, I - invalid
0 name="dhcp1" interface=ether2 lease-time=30m address-
  pool=dhcp_pool0 bootp-support=static authoritative=yes use-
  radius=no lease-script=""

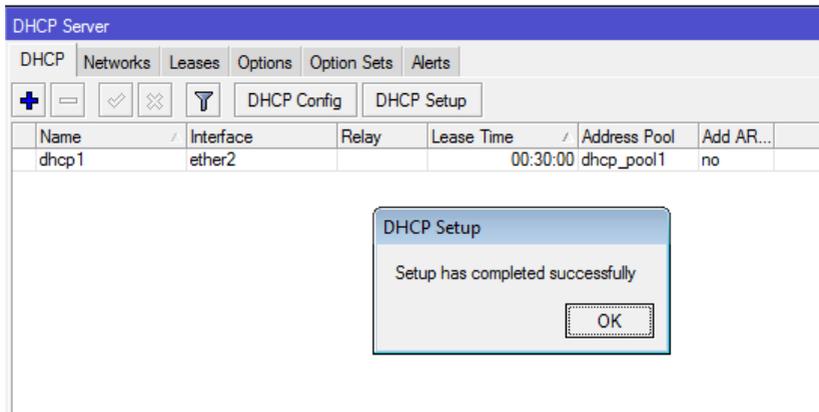
[admin@GATEWAY] > ip dhcp-server network print detail
Flags: D - dynamic
0 address=192.168.1.0/24 gateway=192.168.1.254 dns-
  server=192.168.1.254,1.1.1.254 wins-server="" ntp-server=""
  caps-manager="" dhcp-option=""
```

Jika ingin mengkonfigurasi DHCP Server menggunakan WinBox, maka Anda dapat melakukannya melalui menu **IP → DHCP Server → tab DHCP → tombol DHCP Setup**.



Gambar 3.2
Konfigurasi DHCP Server melalui WinBox

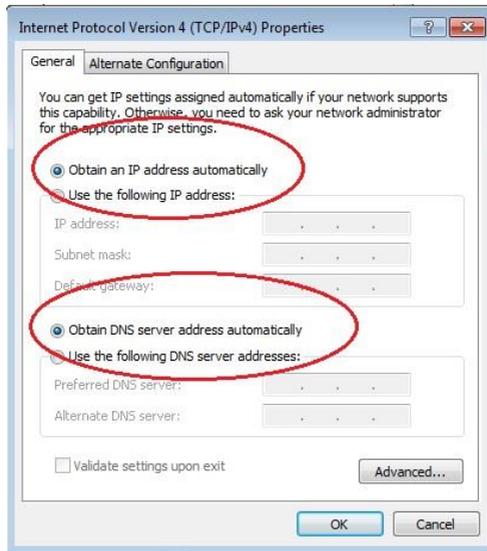
Bila menggunakan WinBox, dan konfigurasi DHCP Server Anda sukses, maka Anda akan mendapati gambar seperti berikut ini.



Gambar 3.3
DHCP Server pada interface *ether2*

Pengujian

Setelah konfigurasi DHCP Server selesai, maka konfigurasi IP Address pada komputer user dapat dikonfigurasi secara otomatis, seperti terlihat pada gambar berikut ini.



Gambar 3.4
Konfigurasi DHCP Client pada Komputer User

Jika komputer user sudah melakukan konfigurasi IP Address secara otomatis, maka pemeriksaan bisa dilanjutkan pada Command Prompt. Pemeriksaan ini bertujuan untuk memastikan apakah komputer user sudah mendapatkan IP Address dari DHCP Server. Perintah yang dapat digunakan pada command prompt adalah perintah *ipconfig /all*, seperti pada gambar berikut ini.

```
Administrator: Command Prompt
C:\Users\admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : admin-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : D0-67-E5-11-00-56
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::35f1:166c:90b9:4d40%11(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 20 Mei 2018 9:26:36
Lease Expires . . . . . : 20 Mei 2018 9:56:36
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 248539109
DHCPv6 Client DUID. . . . . : 00-01-00-01-16-30-96-6A-D0-67-E5-11-00-56

DNS Servers . . . . . : 192.168.1.254
                       1.1.1.254
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\admin>
```

Gambar 3.5
IP Address dari DHCP Server pada Command Prompt

Dari gambar 3.5 terlihat bahwa komputer user mendapatkan IP Address 192.168.1.10 dari DHCP Server. Dan dapat diperhatikan bahwa IP Address tersebut adalah IP Address yang didapatkan dari DHCP (**DHCP Enabled : Yes**). Anda juga dapat melihat bahwa IP Address tersebut dipinjam pada tanggal 20 Mei 2018 jam 09:26:00 dan akan dikembalikan (dilepaskan) oleh komputer user pada tanggal 20 Mei 2018 jam 09:56:36. Informasi lain yang sangat penting adalah siapakah yang bertindak sebagai DHCP Server pada skenario ini. Terlihat bahwa yang bertindak sebagai DHCP Server adalah interface *ether2* dari Router MikroTik (**DHCP Server : 192.168.1.254**)

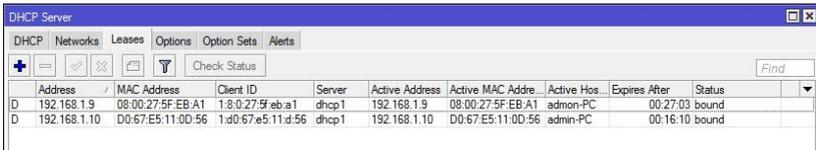
Langkah pengujian selanjutnya dapat dilakukan dari sisi Router MikroTik yang bertindak sebagai DHCP Server. Anda dapat melihat IP Address berapa saja yang sudah dipinjamkan kepada komputer user. Perintah yang dapat digunakan adalah sebagai berikut :

```
[admin@GATEWAY] > ip dhcp-server lease print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
#   ADDRESS          MAC-ADDRESS          HOST-NAME  SERVER  STATUS
0 D 192.168.1.10     D0:67:E5:11:0D:56   admin-PC   dhcp1   bound
1 D 192.168.1.9      08:00:27:5F:EB:A1  admon-PC   dhcp1   bound
```

```
[admin@GATEWAY] > ip dhcp-server lease print detail
Flags: X - disabled, R - radius, D - dynamic, B - blocked
0 D address=192.168.1.10 mac-address=D0:67:E5:11:0D:56 client-
id="1:d0:67:e5:11:d:56" address-lists="" server=dhcp1 dhcp-
option="" status=bound expires-after=18m46s last-
seen=11m14s active-address=192.168.1.10 active-mac-
address=D0:67:E5:11:0D:56 active-client-
id="1:d0:67:e5:11:d:56" active-server=dhcp1 host-
name="admin-PC"

1 D address=192.168.1.9 mac-address=08:00:27:5F:EB:A1 client-
id="1:8:0:27:5f:eb:a1" address-lists="" server=dhcp1 dhcp-
option="" status=bound expires-after=29m39s last-seen=21s
active-address=192.168.1.9 active-mac-
address=08:00:27:5F:EB:A1 active-client-
id="1:8:0:27:5f:eb:a1" active-server=dhcp1 host-
name="admon-PC"
```

Sedangkan jika ingin melihat IP Address berapa saja yang sudah dipinjamkan melalui WinBox, Anda dapat melakukannya melalui menu **IP → DHCP Server → tab Leases**.



Gambar 3.6
IP Address yang sudah dipinjamkan oleh DHCP Server

Static Mapping

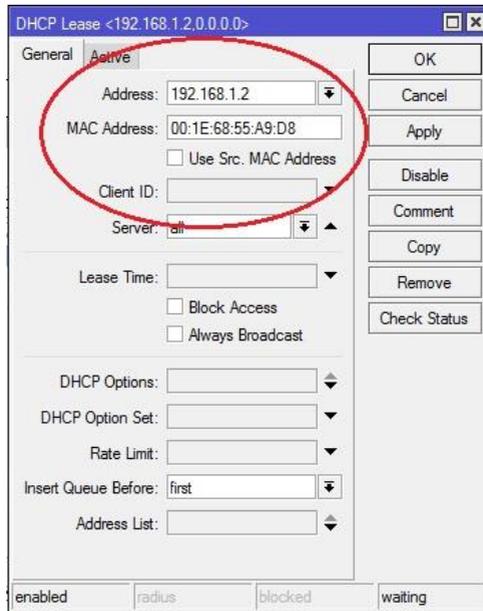
Penerapan DHCP Server akan mengakibatkan setiap komputer user mendapatkan IP Address yang berbeda setiap kali mengajukan peminjaman. Namun DHCP Server dapat meminjamkan IP Address tertentu (atau yang tetap) untuk komputer tertentu berdasarkan MAC Address dari komputer user tersebut. Jadi, IP Address tersebut tidak akan lagi dipinjamkan kepada komputer user yang lain.

Sebagai contoh, jika ada komputer user yang memiliki MAC Address 00:1E:68:55:A9:D8 dan Anda ingin mengalokasikan IP Address 192.168.1.2 pada komputer tersebut, maka perintah yang dapat Anda gunakan adalah sebagai berikut :

```
[admin@GATEWAY] > ip dhcp-server lease add \
address=192.168.1.2 mac-address=00:1E:68:55:A9:D8

[admin@GATEWAY] > ip dhcp-server lease print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
#  ADDRESS      MAC-ADDRESS      HOST-NAME  SERVER  STATUS
0  D 192.168.1.10  D0:67:E5:11:0D:56  admin-PC  dhcp1   bound
1  D 192.168.1.9   08:00:27:5F:EB:A1  admon-PC  dhcp1   bound
2   192.168.1.2   00:1E:68:55:A9:D8                waiting
```

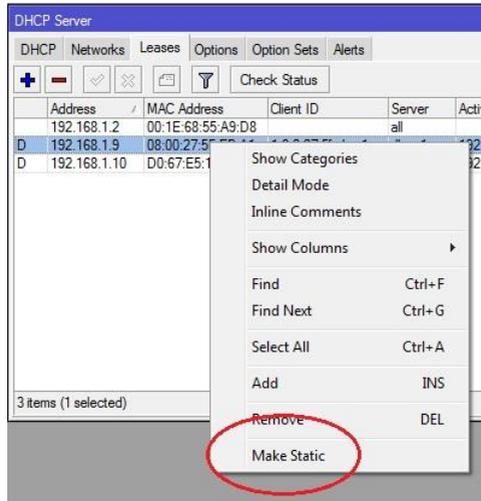
Dengan menggunakan WinBox, Anda dapat melakukannya melalui menu **IP → DHCP Server → tab Leases → tombol Add**, seperti pada gambar berikut :



Gambar 3.7
Pemetaan statik IP Address dan MAC Address melalui WinBox

Jika Anda malas untuk memasukkan MAC Address satu per satu untuk membuat pemetaan statik terhadap IP Address, seperti pada perintah sebelumnya, maka Anda dapat saja menunggu komputer user melakukan peminjaman IP Address seperti biasa. Setelah komputer user tersebut mendapatkan IP Address maka Anda langsung dapat membuat pemetaan statik dengan MAC Address komputer tersebut.

Untuk melakukan pemetaan statik tersebut Anda dapat menggunakan WinBox, melalui menu **IP → DHCP Server → tab Leases →** pilih komputer user yang diinginkan, untuk kemudian melakukan klik kanan dan memilih **Make Static**, seperti pada gambar berikut :



Gambar 3.8
Pemetaan statik antara MAC Address dan IP Address
dengan tombol Make Static

Pengamanan dengan DHCP Server

Sekalipun Anda sudah menyediakan DHCP Server dan membatasi penggunaan IP Address dari 192.168.1.1 s/d 192.168.1.10, namun pengguna jaringan Anda bisa saja jahil dan menggunakan konfigurasi IP Address yang dibuatnya sendiri. Bukankah dia sudah mengetahui bahwa network address Anda adalah 192.168.1.0/24 dengan gateway 192.168.1.254 dan DNS Server juga 192.168.1.254 dan 1.1.1.254. Komputer user yang jahil ini bisa saja mengkonfigurasi IP Address 192.168.1.100, dan ini akan membuat Anda sulit untuk melakukan pengawasan jaringan ☺.

Dengan sedikit tambahan konfigurasi, maka Anda dapat memaksa pengguna jaringan untuk menggunakan DHCP Server. Jika ada komputer user yang berusaha untuk mengkonfigurasi IP Address secara statik, maka user tersebut tidak akan terhubung ke

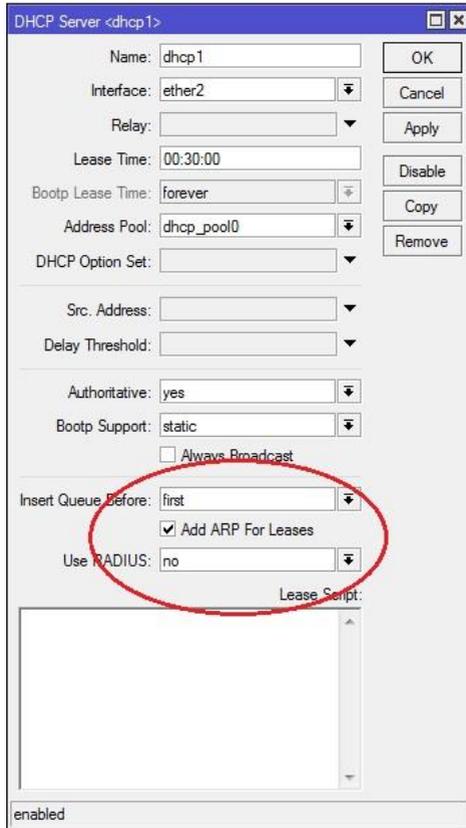
Router MikroTik. Sekalipun dia memakai IP Address 192.168.1.1 s/d 192.168.1.10 !!!

Adapun konfigurasi yang perlu Anda lakukan adalah sebagai berikut :

```
[admin@GATEWAY] > ip dhcp-server print detail
Flags: D - dynamic, X - disabled, I - invalid
0   name="dhcp1" interface=ether2 lease-time=30m address-
    pool=dhcp_pool0 bootp-support=static authoritative=yes use-
    radius=no lease-script=""
```

```
[admin@GATEWAY] > ip dhcp-server set dhcp1 add-arp=yes
```

Dengan menggunakan WinBox, Anda dapat melakukannya melalui menu **IP → DHCP Server → tab DHCP → pilih nama DHCP Server yang sudah dibuat tadi (misalnya *dhcp1*)**, seperti terlihat pada gambar berikut :



Gambar 3.9
Konfigurasi ARP pada DHCP Server

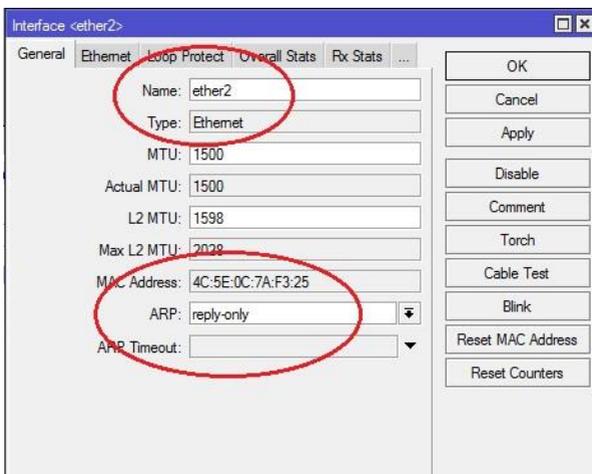
Kemudian lanjutkan konfigurasinya pada interface *ether2* dengan menggunakan perintah berikut :

```
[admin@GATEWAY] > interface ethernet print
Flags: X - disabled, R - running, S - slave
# NAME MTU MAC-ADDRESS ARP SWITCH
0 R ether1 1500 4C:5E:0C:7A:F3:24 enabled SWITCH
1 R ether2 1500 4C:5E:0C:7A:F3:25 enabled switch1
2 X ether3 1500 4C:5E:0C:7A:F3:26 enabled switch1
3 X ether4 1500 4C:5E:0C:7A:F3:27 enabled switch1
4 X ether5 1500 4C:5E:0C:7A:F3:28 enabled switch1

[admin@GATEWAY] > interface ethernet set ether2 arp=reply-only
```

```
[admin@GATEWAY] > interface ethernet print
Flags: X - disabled, R - running, S - slave
#   NAME      MTU  MAC-ADDRESS      ARP           SWITCH
0 R ether1    1500 4C:5E:0C:7A:F3:24 enabled
1 R ether2    1500 4C:5E:0C:7A:F3:25 reply-only    switch1
2 X ether3    1500 4C:5E:0C:7A:F3:26 enabled      switch1
3 X ether4    1500 4C:5E:0C:7A:F3:27 enabled      switch1
4 X ether5    1500 4C:5E:0C:7A:F3:28 enabled      switch1
```

Perintah di atas dapat Anda lakukan dengan menggunakan WinBox melalui menu **Interfaces** → tab **Ethernet** → pilih *ether2*, kemudian melakukan konfigurasi pada tab **General**, seperti pada gambar berikut :



Gambar 3.10
Konfigurasi **ARP reply-only** pada interface *ether2*

End of Chapter

Bab 04

Firewall (Filter)

Konfigurasi yang sudah dibahas pada Bab 2 maupun Bab 3 sudah bisa membuat Router MikroTik memberikan akses Internet kepada komputer user. Dengan bekal konfigurasi yang ada di kedua bab tersebut, sebenarnya Anda sudah berhasil menghubungkan jaringan lokal ke Internet. Namun akses Internet yang diberikan kepada komputer user belum dapat dikendalikan maupun diatur dengan lebih baik.

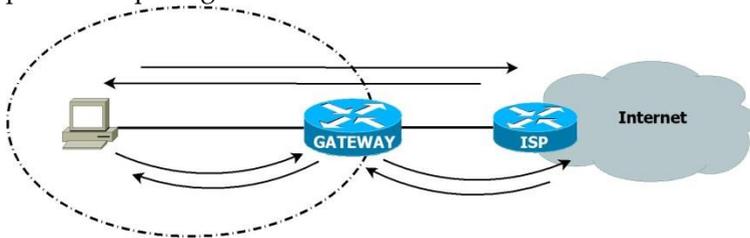
Bisa saja dalam satu jaringan tersebut, Anda hanya menginginkan beberapa komputer saja yang terhubung ke Internet, sedangkan beberapa komputer yang lainnya tidak dapat mengakses Internet. Begitu pula dengan akses ke beberapa website, mungkin saja diinginkan beberapa komputer user tidak bisa mengakses media sosial. Atau bahkan Anda menginginkan akses ke beberapa website hanya bisa diberikan pada jam-jam tertentu.

Untuk mengatur akses Internet sesuai keinginan Anda atau pun sesuai keinginan pemilik jaringan seperti pada contoh di atas, Anda perlu mengaktifkan Firewall pada Router MikroTik. Ada banyak

pengaturan jaringan yang bisa dilakukan oleh Firewall pada Router MikroTik. Namun, untuk pengenalan awal, pada buku ini hanya akan dibahas fungsi Firewall Filter yang ditujukan khusus untuk mengatur akses Internet yang bisa didapatkan oleh komputer user.

Konsep Dasar Firewall

Firewall merupakan fungsi dari sebuah perangkat yang dapat mengatur apakah sebuah paket data bisa keluar dan masuk ke dalam suatu jaringan. Selain itu, Firewall juga dapat menentukan apakah paket data bisa masuk dan keluar ke dalam sebuah router. Berdasarkan arah dan tujuan paket data tadi, maka data dapat dibedakan menjadi paket yang melintasi router, paket yang menuju router maupun paket yang keluar dari dalam router. Ilustrasinya dapat dilihat pada gambar berikut ini.



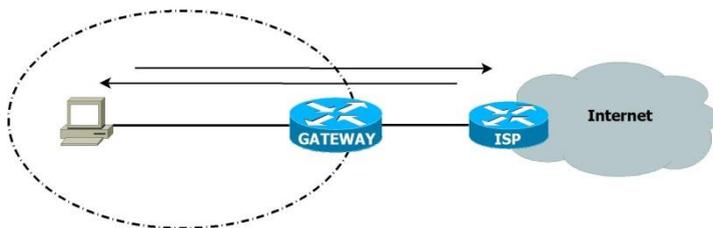
Gambar 4.1

Paket yang melintasi router, menuju router dan keluar dari router

Dari gambar 4.1, terlihat bahwa untuk akses Internet dari komputer user ke Internet (maupun sebaliknya), maka akan dihasilkan paket yang melintasi router. Baik itu melintas dari komputer user ke Internet, maupun dari Internet ke komputer user. Adapun akses komputer user ke Router, misalnya saat Anda mengakses Router MikroTik menggunakan WinBox, maka akan dihasilkan paket yang menuju router. Paket yang menuju router tentunya akan dibalas dengan paket yang keluar dari router. Begitu pula sebaliknya, saat Anda melakukan ping ke salah satu web site di Internet dari New

Terminal WinBox, maka akan dihasilkan paket yang keluar dari router. Tentunya paket yang keluar dari router akan dibalas oleh paket yang menuju ke router.

Karena pembahasan pada bab ini hanya akan mengatur pembatasan akses Internet yang akan diberikan kepada user, maka pembahasan Firewall hanya akan membahas paket yang melintasi router, baik itu dari komputer user ke Internet, maupun sebaliknya.



Gambar 4.2
Paket yang melintasi router

Untuk membatasi akses Internet yang diberikan kepada komputer user maka paket data yang akan dibatasi adalah paket dari komputer user yang menuju ke Internet. Jika paket yang menuju ke Internet sudah dibatasi, tentunya tidak akan ada data balasan dari Internet kepada komputer user.

Chain

Secara default, Firewall Filter pada Router MikroTik memiliki 3 (tiga) parameter *chain*, yang masing-masing adalah sebagai berikut.

- *chain=forward*, chain ini digunakan untuk mengatur paket yang melintasi router. Untuk mengatur akses Internet yang keluar masuk ke dalam jaringan lokal, atau mengatur akses Internet pada komputer user, maka chain ini yang harus digunakan.

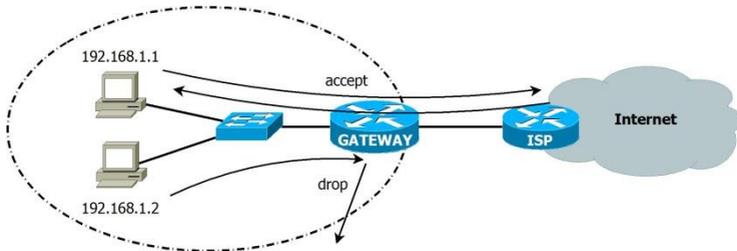
- *chain=input*, chain ini digunakan untuk mengatur packet yang menuju router. Penggunaan chain ini umumnya ditujukan untuk meningkatkan level keamanan dari Router MikroTik itu sendiri.
- *chain=output*, chain ini digunakan untuk mengatur packet yang keluar dari router. Penggunaan chain juga umumnya digunakan untuk meningkatkan level keamanan dari Router MikroTik itu sendiri.

Selain ketiga chain di atas, Anda sebenarnya dapat membuat chain sesuai kebutuhan konfigurasi. Namun, untuk pembahasan pada buku ini chain yang digunakan hanyalah chain *forward*. Pembahasan Firewall pada buku ini hanya ditujukan untuk mengatur akses Internet yang akan diberikan kepada komputer user. Untuk pengamanan Router MikroTik itu sendiri dan konfigurasi yang lebih rumit belum akan dibahas pada buku ini.

Action

Pada saat akan melakukan konfigurasi Firewall Filter, terdapat parameter *action* yang bisa menentukan apakah sebuah paket akan diloloskan untuk menuju Internet, ataukah paket tersebut harus dibuang sehingga tidak mencapai Internet. Ada banyak nilai yang bisa digunakan pada parameter *action* ini, namun untuk pengenalan awal Firewall Filter, hanya akan dibahas 3 (tiga) jenis parameter *action*, masing-masing sebagai berikut.

- *action=accept*, action ini dapat digunakan untuk meloloskan paket data yang akan menuju Internet.
- *action=drop*, action ini dapat digunakan untuk membuang paket data yang akan menuju Internet. Action ini tidak akan memberikan pemberitahuan (notifikasi) kepada komputer user.
- *action=reject*, action ini memiliki fungsi yang sama dengan *action=drop*, namun action ini akan mengirimkan pesan error kepada komputer user, sehingga user bisa mengetahui bahwa paket datanya telah ditolak oleh firewall.



Gambar 4.3
Penggunaan action pada Firewall Filter

Dari gambar 4.3, terlihat bahwa Firewall Filter pada Router Gateway membuang (drop) paket dari komputer 192.168.1.2. Sedangkan paket dari komputer 192.168.1.1 diloloskan menuju Internet. Ini mengakibatkan komputer 192.168.1.1 bisa mengakses Internet, sedangkan komputer 192.168.1.2 tidak akan bisa mendapatkan akses Internet.

Ada banyak parameter *action* yang dapat digunakan untuk meningkatkan level keamanan dari suatu jaringan. Penggunaan action-action tersebut akan dibahas pada buku yang lain.

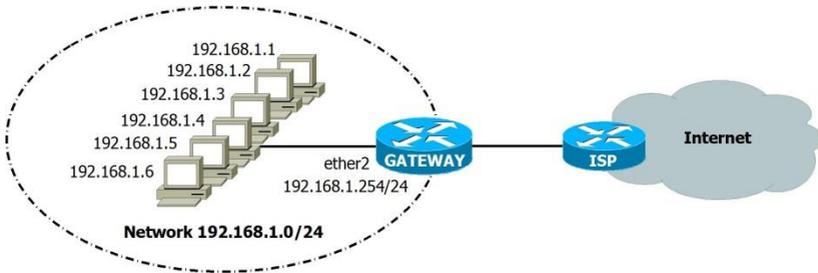
Top to Bottom

Keseluruhan konfigurasi Firewall nantinya akan tersusun dari beberapa konfigurasi atau rule-rule. Beberapa rule tersebut akan dijalankan oleh Router MikroTik dengan menggunakan prinsip *top to bottom* (akan dijalankan dari atas ke bawah). Sehingga, bila konfigurasi Firewall terdiri dari beberapa rule, maka susunan rule-rule tersebut akan sangat menentukan efektif tidaknya skenario Firewall Filter yang diinginkan.

Pentingnya susunan konfigurasi Firewall akan dibahas pada bagian Best Practice atau bagian latihan yang ada pada sub bab selanjutnya.

Topologi

Adapun topologi yang akan digunakan pada Bab Firewall Filter ini dapat dilihat pada gambar berikut ini.



Gambar 4.4
Router Gateway melakukan filter berdasarkan IP Address user

Dari gambar 4.4, terlihat Router Gateway yang bertugas sebagai Internet Gateway bagi jaringan 192.168.1.0/24. Pada jaringan tersebut terdapat beberapa komputer user yang menggunakan IP Address 192.168.1.1, 192.168.1.2 dan seterusnya. Asumsi yang digunakan adalah Router Gateway yang sudah melakukan konfigurasi IP Address pada interface *ether1* maupun *ether2*, sudah melakukan konfigurasi default route, sudah melakukan konfigurasi DNS Server dan sudah melakukan konfigurasi Firewall masquerade, sudah melakukan konfigurasi DHCP Server, sehingga semua user pada jaringan 192.168.1.0/24 sudah bisa mengakses Internet. Asumsi konfigurasi ini adalah konfigurasi yang sudah dibahas pada bab-bab sebelumnya.

Filter Berdasarkan IP Address

Pada dasarnya Firewall Filter bekerja berdasarkan IP Address, baik itu yang digunakan oleh komputer user maupun IP Address yang digunakan web site atau server-server di Internet. Untuk membatasi

akses Internet yang bisa didapatkan oleh user, maka Firewall Filter harus bekerja berdasarkan IP Address yang digunakan pada komputer user. Pada sub bab ini akan dibahas konfigurasi Firewall yang bekerja berdasarkan IP Address komputer user dan juga bekerja berdasarkan waktu.

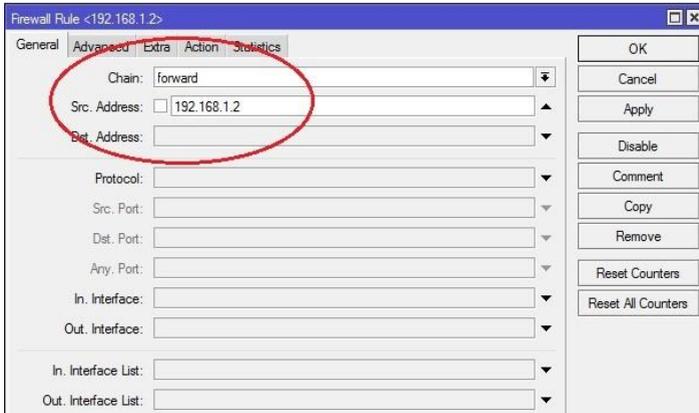
Parameter *src-address*

Untuk membatasi akses Internet pada komputer user berdasarkan IP Address, maka konfigurasi Firewall Filter perlu dilakukan dengan menggunakan parameter *src-address* (IP Address pengirim). Sebagai contoh, jika diinginkan user dengan IP Address 192.168.1.2 tidak bisa mengakses Internet, maka perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.2 action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=drop src-address=192.168.1.2
```

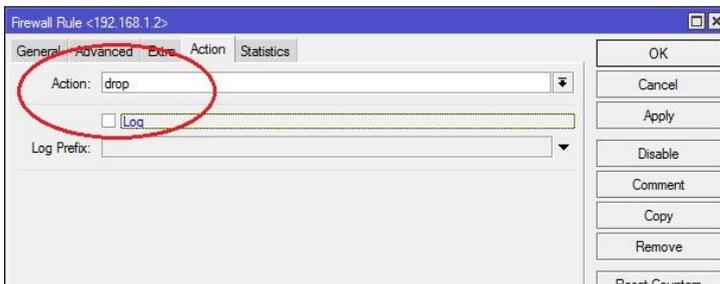
Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Firewall → tab Filter Rules**, tombol **Add**, seperti terlihat pada gambar berikut ini.



Gambar 4.5

Konfigurasi Firewall Filter untuk komputer 192.168.1.2

Untuk parameter *action=drop* dapat dikonfigurasi pada tab **Action**.



Gambar 4.6

Parameter **action=drop** pada tab Action

Penggunaan parameter *action=drop* bisa saja Anda ganti dengan menggunakan parameter *action=reject*. Hasil akhir yang didapatkan adalah sama, keduanya akan membuat komputer user tidak bisa mendapatkan akses Internet.

Jika dikemudian hari diinginkan user 192.168.1.3 juga tidak bisa mengakses Internet, maka perintah yang sudah ada sebelumnya dapat ditambahkan seperti terlihat pada uraian berikut ini.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.3 action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=drop src-address=192.168.1.2

1 chain=forward action=drop src-address=192.168.1.3
```

Jika diinginkan pembatasan dilakukan untuk beberapa user, misalnya komputer dengan IP Address 192.168.1.11 s/d 192.168.1.20, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.11-192.168.1.20 action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=drop src-address=192.168.1.2

1 chain=forward action=drop src-address=192.168.1.3

2 chain=forward action=drop src-address=192.168.1.11-
192.168.1.20
```

Penggunaan prefix pada parameter *src-address* juga bisa diterapkan, misalnya saja ingin melakukan pembatasan akses Internet untuk komputer dengan IP Address 192.168.1.1 s/d 192.168.1.63, maka penggunaan parameter *src-address* bisa saja menggunakan nilai 192.168.1.0/26, seperti uraian berikut ini.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.0/26 action=drop
```

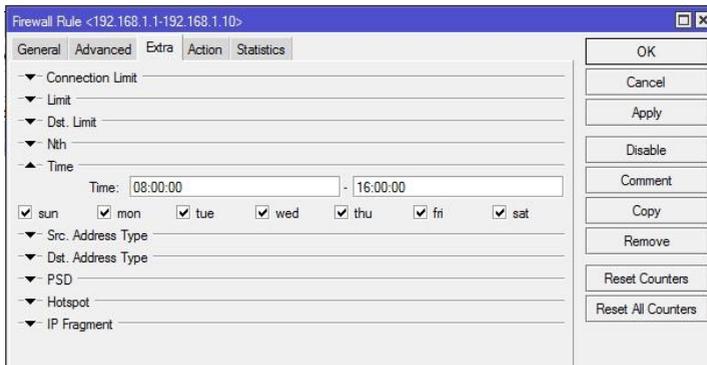
Parameter time

Parameter *time* bisa dimanfaatkan untuk melakukan pembatasan akses Internet berdasarkan waktu. Misalnya saja diinginkan komputer dengan IP Address 192.168.1.1 s/d 192.168.1.10 tidak bisa mengakses Internet pada jam 08.00 s.d 16.00 setiap harinya, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1-192.168.1.10 \
time=08:00:00-16:00:00,mon,tue,wed,thu,fri,sat,sun \
action=drop
```

```
[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 I   ;; inactive time
      chain=forward action=drop src-address=192.168.1.1-
      192.168.1.10 time=8h-16h,sun,mon,tue,wed,thu,fri,sat
```

Bila menggunakan WinBox, parameter *time* dapat dikonfigurasi pada tab **Extra**, seperti terlihat pada gambar berikut ini.



Gambar 4.7
Parameter *time* pada tab **Extra**

Sebagai catatan, saat Anda menggunakan konfigurasi Firewall dan menggunakan parameter *time*, maka pada waktu konfigurasi tersebut belum diaktifkan, konfigurasi tersebut akan diberi keterangan *-inactive time*. Ini menunjukkan bahwa konfigurasi

tersebut hadir dalam Firewall Filter namun belum bekerja, karena belum diijinkan oleh parameter *time*.

Best Practice

Pada bagian ini akan dibahas sebuah skenario manajemen jaringan yang dilakukan berdasarkan IP Address komputer user dan juga berdasarkan waktu. Skenario jaringan yang digunakan adalah sebuah jaringan dengan network address 192.168.1.0/24, seperti pada gambar 4.4. Jaringan tersebut terdiri dari 10 (sepuluh) unit komputer user, masing-masing dengan IP Address 192.168.1.1 s/d 192.168.1.10.

Adapun skenario manajemen pembatasan akses Internet yang diinginkan adalah sebagai berikut.

1. Komputer dengan IP Address 192.168.1.1 s/d 192.168.1.5 akan mendapatkan akses Internet sepanjang hari dan sepanjang waktu.
2. Komputer dengan IP Address 192.168.1.6 s/d 192.168.1.10 hanya mendapatkan akses Internet selama hari kerja dan jam kerja.
3. Adapun hari kerja adalah hari Senin s/d Jum'at, sedangkan jam kerja adalah 08.00 s/d 16.30.
4. Harus dipastikan bahwa tidak ada komputer lain yang bisa mendapatkan akses Internet. Dengan kata lain, jika terdapat komputer dengan IP Address 192.168.1.11 s/d 192.168.1.255, maka komputer-komputer tersebut tidak akan terhubung ke Internet.

Adapun perintah yang dapat digunakan untuk mewujudkan skenario Best Practice ini dapat dijabarkan sebagai berikut.

Untuk memberikan akses Internet sepanjang waktu untuk user 192.168.1.1 s/d 192.168.1.5, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1-192.168.1.5 action=accept
```

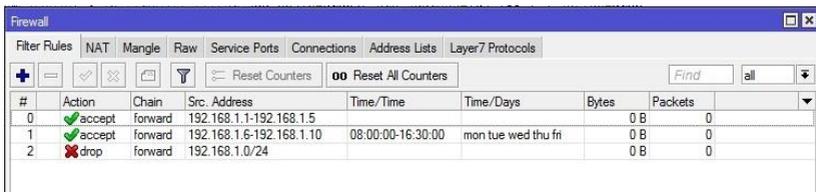
Untuk memberikan akses Internet selama hari kerja dan jam kerja bagi user 192.168.1.6 s/d 192.168.1.10, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.6-192.168.1.10 \
time=08:00:00-16:30:00,mon,tue,wed,thu,fri action=accept
```

Sedangkan untuk mencegah user dengan IP Address 192.168.1.11 s/d 192.168.1.254 mendapatkan akses Internet, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.0/24 action=drop
```

Setelah konfigurasi tersebut selesai, maka menu **IP → Firewall → tab Filter Rules** pada WinBox, akan terlihat seperti gambar berikut ini.



#	Action	Chain	Src. Address	Time/Time	Time/Days	Bytes	Packets
0	✓ accept	forward	192.168.1.1-192.168.1.5			0 B	0
1	✓ accept	forward	192.168.1.6-192.168.1.10	08:00:00-16:30:00	mon tue wed thu fri	0 B	0
2	✗ drop	forward	192.168.1.0/24			0 B	0

Gambar 4.8
Konfigurasi Firewall untuk network 192.168.1.0/24

Sebagai catatan, karena susunan rule pada Firewall sangat penting, maka susunan rule tersebut harus sesuai dengan gambar 4.8. Jangan sampai Anda menempatkan rule dengan parameter *src-address=192.168.1.0/24* dengan *action=drop* menjadi rule yang paling pertama seperti pada tampilan berikut ini.

#	Action	Chain	Src. Address	Time/Time	Time/Days	Bytes	Packets
0	✗ drop	forward	192.168.1.0/24			0 B	0
1	✓ accept	forward	192.168.1.1-192.168.1.5			0 B	0
2	✓ accept	forward	192.168.1.6-192.168.1.10	08:00:00-16:30:00	mon tue wed thu fri	0 B	0

Gambar 4.9

Rule dengan `src-address=192.168.1.0/24` berada paling atas

Jika ternyata Anda menempatkan rule-rule Firewall Filter seperti pada gambar 4.9, maka bisa dipastikan tidak ada satu pun komputer pada jaringan tersebut yang bisa mengakses Internet. Ini karena baris pertama sudah menyatakan bahwa semua komputer pada jaringan 192.168.1.0/24 tidak bisa mendapatkan akses Internet. Penempatan rule dengan `src-address=192.168.1.0/24` `action=drop` akan membuat rule dengan `src-address=192.168.1.1-192.168.1.5` tidak akan dijalankan lagi oleh Firewall Filter. Begitu pula dengan rule yang menggunakan `src-address=192.168.1.6-192.168.1.11`, rule ini tidak akan dijalankan lagi karena sudah didahului oleh rule dengan `src-address=192.168.1.0/24`. Bukankah rentang IP Address 192.168.1.1-192.168.1.5 dan 192.168.1.6-192.168.1.10 merupakan bagian dari 192.168.1.0/24. Dan saat Anda menyatakan 192.168.1.0/24 itu berarti Anda turut menyatakan IP Address 192.168.1.1 s/d 192.168.1.254.

Untuk memindahkan urutan rule pada firewall, Anda dapat menggunakan cara *drag n drop* terhadap rule konfigurasi firewall pada WinBox.

Sebagai catatan, konfigurasi Firewall adalah konfigurasi logika. Sehingga untuk mencapai suatu tujuan skenario pembatasan akses bagi komputer user, Anda bisa saja membuat konfigurasi yang berbeda dengan apa yang ada pada pembahasan bab ini.

Filter Services

Internet saat ini menyediakan berbagai layanan (services), mulai dari layanan yang dikenal luas sampai dengan berbagai layanan khusus yang hanya digunakan sebagian user. Mulai dari layanan browsing (HTTP dan HTTPS), layanan DNS, layanan Proxy sampai dengan layanan Virtual Private Network (VPN) yang sering digunakan untuk mengakses konten-konten terlarang ☺.

Pada sub bab ini akan dibahas konfigurasi-konfigurasi yang ditujukan untuk membatasi akses Internet berdasarkan layanan yang akan diberikan. Untuk membatasi berbagai layanan Internet sangat dibutuhkan pengetahuan tentang nomor port (**port number**) beserta **protocol** yang digunakan layanan tersebut. Untuk mendalami pengetahuan tentang **port number** dan **protocol**, sangat disarankan untuk membaca buku-buku tentang TCP/IP. Namun, bagi Anda yang belum mahir ilmu TCP/IP, beberapa konfigurasi sederhana pada sub bab ini bisa menjadi acuan untuk memecahkan berbagai skenario firewall yang mungkin Anda temui.

Adapun asumsi topologi yang digunakan pada sub bab ini, adalah topologi jaringan yang sama dengan sub bab sebelumnya, seperti terlihat pada gambar 4.4.

Filter HTTP dan HTTPS

Untuk membatasi akses browsing HTTP, rule firewall harus menggunakan parameter *protocol=tcp* dan *dst-port=80*. Adapun untuk akses HTTPS, parameter yang digunakan adalah *protocol=tcp* dan *dst-port=443*.

Sebagai contoh, jika akses browsing (HTTP dan HTTPS) tidak akan diberikan kepada komputer 192.168.1.2, maka perintah yang dapat digunakan adalah sebagai berikut

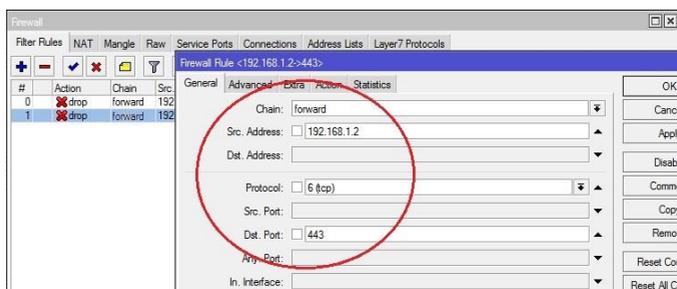
```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.2 protocol=tcp dst-port=80 action=drop
```

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.2 protocol=tcp dst-port=443 action=drop
```

```
[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=drop protocol=tcp src-
address=192.168.1.2 dst-port=80

1 chain=forward action=drop protocol=tcp src-
address=192.168.1.2 dst-port=443
```

Dengan menggunakan WinBox, parameter *protocol* dan *dst-port* dapat dikonfigurasi pada menu **IP → Firewall → tab Filter Rules** → tombol **Add** → tab **General**, seperti pada gambar berikut ini.



Gambar 4.10

Parameter *protocol* dan *dst-port*

Sebenarnya, kedua rule firewall yang masing-masing menggunakan parameter *dst-port=80* dan *dst-port=443* dapat digabung menjadi satu konfigurasi saja dengan perintah seperti berikut ini.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.2 protocol=tcp dst-port=80,443 \
action=drop
```

```
[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=drop protocol=tcp src-
address=192.168.1.2 dst-port=80,443
```

Filter Domain Name System (DNS)

Terkadang beberapa user sering menggunakan DNS Server terbuka untuk mengakses konten-konten terlarang. Untuk kondisi ini, Anda harus melakukan konfigurasi Firewall Filter sehingga komputer user harus dipaksa menggunakan DNS Server yang sudah dijalankan pada Router MikroTik. Tentunya untuk menggunakan DNS Server (DNS Caching) ini, parameter *allow-remote-request=yes* pada konfigurasi DNS harus digunakan.

Layanan DNS menggunakan protocol UDP dengan port number 53, sehingga saat membuat rule untuk membatasi akses DNS, parameter yang digunakan adalah *protocol=udp* dan *dst-port=53*.

Sebagai contoh, jika diinginkan semua komputer dalam jaringan lokal 192.168.1.0/24 tidak bisa menggunakan akses DNS selain DNS Server pada Router MikroTik, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.0/24 protocol=udp dst-port=53 \
action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=forward action=drop protocol=udp src-
address=192.168.1.0/24 dst-port=53
```

Best Practice

Asumsi topologi yang digunakan pada bagian ini adalah topologi pada gambar 4.4. Jaringan tersebut terdiri dari 10 (sepuluh) unit komputer user, masing-masing dengan IP Address 192.168.1.1 s/d 192.168.1.10.

Adapun skenario manajemen pembatasan akses yang diinginkan adalah sebagai berikut.

1. User yang bisa mendapatkan layanan Internet adalah komputer dengan IP Address 192.168.1.1 s/d 192.168.1.10. Komputer selain dengan IP Address tersebut tidak bisa mendapatkan akses Internet.
2. Jika ingin menggunakan DNS, maka akses DNS hanya diperkenankan menggunakan layanan DNS dari Router MikroTik. Tidak diperkenankan menggunakan layanan DNS terbuka yang berada di Internet.
3. Layanan Internet yang diberikan hanyalah layanan HTTP dan HTTPS. Selain kedua layanan itu, harus dipastikan tidak ada layanan lain yang diberikan, sehingga komputer dengan IP Address 192.168.1.1 s/d 192.168.1.10 tidak bisa menggunakan layanan Proxy maupun VPN yang berada di Internet.

Untuk mewujudkan skenario di atas, maka contoh perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1-192.168.1.10 protocol=tcp \
dst-port=80,443 action=accept

[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.0/24 action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=forward action=accept protocol=tcp src-
  address=192.168.1.1-192.168.1.10 dst-port=80,443

 1 chain=forward action=drop src-address=192.168.1.0/24
```

Setelah konfigurasi selesai dilakukan, maka harus dipastikan bahwa susunan rule pada Firewall akan terlihat seperti gambar berikut ini.

Firewall								
Filter Rules								
#	Action	Chain	Src. Address	Protocol	Dst. Port	Bytes	Packets	
0	accept	forward	192.168.1.1-192.168.1.10	6 (tcp)	80,443	117.4 KiB	704	
1	drop	forward	192.168.1.0/24			874 B	19	

Gambar 4.11
Susunan rule firewall untuk browsing dan DNS

Dari uraian dan gambar 4.11, rule yang pertama adalah konfigurasi yang mengizinkan komputer 192.168.1.1 s/d 192.168.1.10 untuk mengakses Internet. Akses Internet yang diberikan hanyalah akses browsing HTTP dan HTTPS. Adapun akses DNS, Proxy, VPN dan lain-lain tidak akan diijinkan. Adapun rule kedua bertugas untuk memastikan tidak ada komputer lain (selain 192.168.1.1-192.168.1.10) yang bisa mengakses Internet. Rule kedua ini pula bertugas untuk menjamin tidak ada layanan Internet lain yang akan diberikan, selain tentunya akses HTTP/HTTPS yang sudah diberikan oleh rule pertama.

Sebagai tambahan latihan, jika suatu hari diinginkan komputer 192.168.1.1 diberikan pengecualian, misalnya saja komputer ini bisa saja mengakses apa saja, baik itu HTTP, HTTPS, DNS, Proxy maupun akses VPN yang berada di Internet, maka perintah berikut ini dapat ditambahkan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1 action=accept

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=accept protocol=tcp src-
address=192.168.1.1-192.168.1.10 dst-port=80,443

1 chain=forward action=drop src-address=192.168.1.0/24
log=no log-prefix=""

2 chain=forward action=accept src-address=192.168.1.1
```

Rule yang baru ditambahkan tadi, harus dipastikan berada pada susunan paling atas, sehingga akses Internet kepada komputer 192.168.1.1 tersebut dapat diberikan terlebih dahulu. Untuk memindahkan rule tersebut, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter move 2 0

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=accept src-address=192.168.1.1

 1   chain=forward action=accept protocol=tcp src-
     address=192.168.1.1-192.168.1.10 dst-port=80,443

 2   chain=forward action=drop src-address=192.168.1.0/24
     log=no log-prefix=""
```

Setelah dilakukan pemindahan rule, maka susunan konfigurasi Firewall Filter untuk pengecualian komputer 192.168.1.1 seharusnya terlihat seperti pada gambar berikut ini.

#	Action	Chain	Src. Address	Protocol	Dst. Port	Bytes	Packets
0	✓ accept	forward	192.168.1.1			0 B	0
1	✓ accept	forward	192.168.1.1-192.168.1.10	6 (tcp)	80,443	235.6 KiB	1 033
2	✗ drop	forward	192.168.1.0/24			4294 B	89

Gambar 4.12
Susunan Firewall Filter untuk komputer 192.168.1.1

Filter Website

Firewall Router MikroTik memiliki parameter **Content** dan **L7 Protocol** yang dapat digunakan membatasi akses Internet untuk website-website tertentu saja. Kedua parameter tersebut juga dapat digunakan untuk membatasi ekstensi file yang bisa di-download oleh komputer user.

Asumsi yang digunakan pada sub bab ini adalah topologi yang ada pada gambar 4.4.

Filter dengan Content

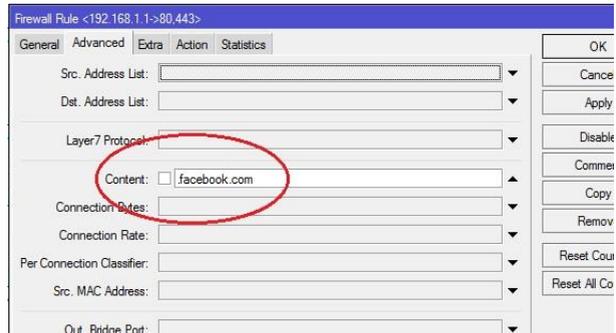
Sebagai contoh penggunaan parameter *content*, jika diinginkan komputer 192.168.1.1 tidak bisa mengakses media sosial seperti Facebook, maka perintah berikut ini dapat digunakan, perhatikanlah parameter *content=.facebook.com*

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1 protocol=tcp dst-port=80,443 \
content=.facebook.com action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=forward action=drop protocol=tcp src-
  address=192.168.1.1 dst-port=80,443 content=.facebook.com
```

Dengan menggunakan WinBox, parameter *content* dapat dikonfigurasi pada tab **Advanced**, seperti terlihat pada gambar berikut ini.

Gambar 4.13
Parameter *content*



Sebagai contoh tambahan, jika ingin melakukan pembatasan jenis ekstensi file yang tidak bisa di-download dari Internet, maka contoh berikut ini memperlihatkan bahwa komputer 192.168.1.1 tidak bisa melakukan download file dengan ekstensi .mp4 dari Internet.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1 protocol=tcp dst-port=80,443 \
content=.mp4 action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=drop protocol=tcp src-
address=192.168.1.1 dst-port=80,443 content=.facebook.com

1 chain=forward action=drop protocol=tcp src-
address=192.168.1.1 dst-port=80,443 content=.mp4
```

Sebagai catatan penting, terkadang konfigurasi pembatasan akses terhadap beberapa website tidak langsung dijalankan oleh Router Mikrotik. Terkadang harus dilakukan prosedur restart router agar status koneksi yang mungkin sempat terjalin (**established**) ke website tersebut bisa hilang dan pembatasan akses akan bekerja.

Filter dengan L7 Protocol

Untuk menggunakan parameter L7 Protocol pada Firewall Filter, maka terlebih dahulu harus dibuat Regular Expression pada bagian L7 Protocol. Sebagai contoh untuk membatasi akses Youtube maka

Anda dapat mencoba Regular Expression yang diambil dari alamat <https://dokter-squid.com> berikut ini.

r[0-9]+---[a-z]+++[a-z0-9-]+\.\googlevideo\.com

Regular Expression tersebut dapat ditambahkan pada menu **IP → Firewall → tab L7 Protocols**, tombol **Add**, seperti pada gambar berikut ini.



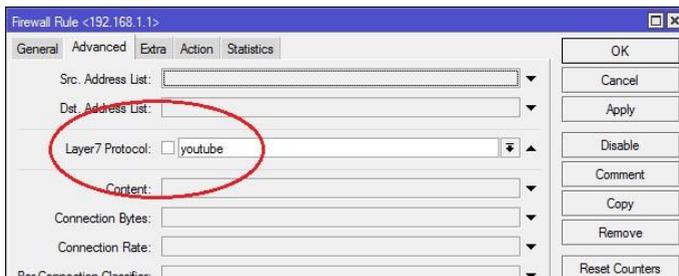
Gambar 4.14
Layer 7 Protocols pada Firewall

Selanjutnya, jika pembatasan web site dengan L7 Protocols akan diterapkan pada user 192.168.1.1, maka perintah berikut ini dapat digunakan. Perhatikanlah penggunaan parameter *l7-protocols=youtube*.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1 layer7-protocol=youtube \
action=drop

[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward action=drop layer7-protocol=youtube src-
address=192.168.1.1
```

Dengan menggunakan WinBox, parameter *l7-protocols* dapat dikonfigurasi pada tab **Advanced**, seperti terlihat pada gambar berikut ini.



Gambar 4.15
Parameter *l7-protocols* pada Firewall Filter

Best Practice

Asumsi topologi yang digunakan pada bagian ini adalah topologi pada gambar 4.4. Jaringan tersebut terdiri dari 10 (sepuluh) unit komputer user, masing-masing dengan IP Address 192.168.1.1 s/d 192.168.1.10.

Adapun skenario pembatasan akses Internet yang diinginkan adalah sebagai berikut.

1. Komputer yang bisa mendapatkan layanan Internet adalah komputer dengan IP Address 192.168.1.1 s/d 192.168.1.10, sepanjang hari dan sepanjang waktu.
2. Namun, komputer dengan IP Address 192.168.1.1 s/d 192.168.1.7 tidak dapat mengakses media sosial Facebook selama hari kerja dan jam kerja. Hari kerja adalah hari Senin s/d Jumat sedangkan jam kerja adalah 08.00 s/d 16.30.

3. Selain komputer 192.168.1.1 s/d 192.168.1.10, tidak akan bisa mengakses Internet. Dengan kata lain, komputer 192.168.1.11 s/d 192.168.1.254 tidak bisa mengakses Internet.

Untuk mewujudkan skenario di atas, maka langkah konfigurasi yang dapat dilakukan adalah membatasi terlebih dahulu akses Facebook terhadap komputer 192.168.1.1 s/d 192.168.1.7, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1-192.168.1.7 protocol=tcp \
dst-port=80,443 content=.facebook.com \
time=08:00:00-16:30:00,mon,tue,wed,thu,fri action=drop
```

Selanjutnya, untuk memberikan semua layanan Internet kepada 10 unit komputer (192.168.1.1 s/d 192.168.1.10), maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.1-192.168.1.10 action=accept
```

Sedangkan untuk memastikan tidak ada komputer lain (selain 10 unit komputer tersebut) yang dapat menggunakan akses Internet, maka perintah berikut ini dapat ditambahkan.

```
[admin@GATEWAY] > ip firewall filter add chain=forward \
src-address=192.168.1.0/24 action=drop
```

```
[admin@GATEWAY] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=forward action=drop protocol=tcp src-
  address=192.168.1.1-192.168.1.7 dst-port=80,443
  content=.facebook.com time=8h-16h30m,mon,tue,wed,thu,fri

 1 chain=forward action=accept src-address=192.168.1.1-
 192.168.1.10

 2 chain=forward action=drop src-address=192.168.1.0/24
```

Setelah konfigurasi selesai dilakukan, maka susunan rule pada Firewall Filter seharusnya terlihat seperti gambar berikut ini.

#	Action	Chain	Src. Address	Protocol	Dest. Port	Content	Time/Time	Time/Days
0	drop	forward	192.168.1.1-192.168.1.7	6 (tcp)	80,443	facebook.com	08:00:00-16:30:00	mon tue wed thu fri
1	accept	forward	192.168.1.1-192.168.1.10					
2	drop	forward	192.168.1.0/24					

Gambar 4.16
Konfigurasi Firewall Filter untuk menutup Facebook

Yang harus diperhatikan dari konfigurasi tadi adalah susunan rule-rule dari Firewall Filter. Harus dipastikan bahwa rule yang menutup akses Facebook berada pada susunan teratas. Jika rule tersebut berada sesudah rule yang memberikan akses Internet kepada komputer 192.168.1.1 s/d 192.168.1.10, maka rule pembatasan Facebook tersebut tidak akan bekerja. Ini karena sepuluh unit komputer tersebut (termasuk komputer 192.168.1.1 s/d 192.168.1.7) sudah mendapatkan akses Internet tanpa batas terlebih dahulu. Dengan kata lain, pembatasan Facebook tidak akan berhasil, ini karena Firewall Filter ternyata sudah membebaskan akses Internet terlebih dahulu, dan Anda baru menginginkan akses ke Facebook ditutup, sesuatu yang sulit dilakukan oleh Firewall karena Firewall Filter akan membaca rule-rule tersebut dari atas ke bawah (*top to bottom*).

End of Chapter

Bab 05

Wireless Network

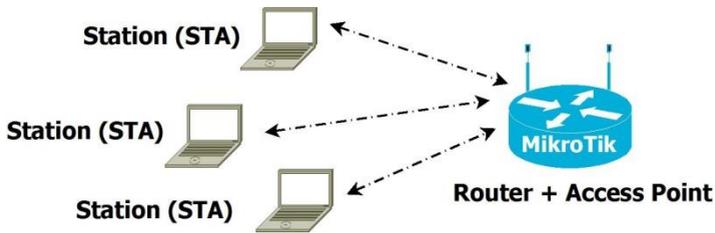
Untuk memberikan layanan Internet kepada pengguna (user) yang memiliki laptop maupun smartphone, Router MikroTik harus menyediakan akses jaringan nirkabel atau jaringan wireless. Untuk Router MikroTik yang memiliki interface wireless, seperti router yang digunakan sebagai acuan pada buku ini, maka jaringan wireless yang diinginkan akan bisa langsung diterapkan. Sedangkan untuk router yang tidak memiliki interface wireless, maka dibutuhkan tambahan perangkat Access Point, baik itu Access Point MikroTik maupun Access Point dari pabrikan lain.

Jaringan wireless memiliki infrastruktur yang berbeda dengan jaringan kabel. Jaringan wireless membutuhkan gelombang elektromagnetik untuk mengirimkan paket data melalui udara. Untuk itu, dibutuhkan sedikit pemahaman tentang teori jaringan wireless sebelum Anda melakukan konfigurasi di lapangan. Ada banyak teori yang membahas tentang jaringan wireless, namun untuk kebutuhan buku ini, yang akan dibahas adalah teori mendasar.

Konsep Dasar Wireless Network

Jaringan wireless adalah jaringan yang dibangun dengan memanfaatkan udara sebagai media pengiriman data. Data yang akan dikirimkan akan diubah menjadi gelombang elektromagnetik sehingga dapat dengan mudah dikirimkan melalui udara. Untuk mengubah data yang biasanya dikirimkan melalui kabel sehingga menjadi gelombang elektromagnetik dibutuhkan perangkat khusus yang disebut Access Point. Para teknisi di lapangan sering menyebut perangkat ini sebagai “radio”, karena memang perangkat tersebut akan memancarkan gelombang radio elektromagnetik.

Jaringan wireless dibangun dengan melibatkan setidaknya 2 (dua) perangkat, masing-masing adalah perangkat Access Point (AP) dan perangkat Station (STA). Untuk jaringan wireless sederhana, umumnya dibangun dengan menggunakan 1 (satu) buah Access Point dan beberapa laptop/smartphone yang bertindak sebagai Station. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 5.1
Implementasi jaringan wireless

Dari gambar 5.1, Router MikroTik memiliki interface wireless. Dengan demikian jaringan wireless akan langsung dapat dibangun dengan mengaktifkan dan melakukan konfigurasi pada interface wireless (*wlan*) pada router tersebut. Dengan kata lain, jaringan wireless pada gambar 5.1 akan langsung dapat dibangun dengan mengfungsikan Router MikroTik sebagai Access Point. Dari gambar tersebut, juga terlihat bahwa signal elektromagnetik yang

dipancarkan oleh Router MikroTik akan ditangkap oleh beberapa unit laptop. Pada kondisi ini, laptop merupakan perangkat yang bertindak sebagai Station (STA). Nantinya, perangkat laptop akan mendapatkan akses Internet jika berhasil menangkap signal yang dipancarkan oleh Access Point.

Setidaknya ada 4 (empat) parameter mendasar yang harus dikonfigurasi sehingga interface wireless pada Router MikroTik bisa bertindak sebagai Access Point. Keempat parameter tersebut adalah *mode*, *band*, *frequency* dan *ssid*.

Mode

Mode merupakan parameter pertama yang harus dikonfigurasi pada interface wireless. Saat akan menjadikan Router MikroTik sebagai Access Point, maka Anda harus menggunakan parameter *mode=ap-bridge*. Router MikroTik sebenarnya bisa bertugas sebagai Station pula, maupun bertugas sebagai perangkat lain seperti Repeater. Namun, pada buku ini parameter yang digunakan adalah parameter *mode=ap-bridge* yang memang ditujukan untuk menjadikan interface wireless sebagai Access Point.

Band

Band merupakan parameter yang bisa menentukan standar spesifikasi apa yang akan dijalankan oleh interface wireless pada Router MikroTik. Juga akan menentukan pada rentang frekuensi berapakah Access Point tersebut akan memancarkan signal elektromagnetik. Spesifikasi jaringan wireless yang diimplementasikan saat ini adalah standar 802.11a, 802.11b, 802.11g, 802.11n dan 802.11ac.

Parameter *band* juga menentukan rentang frekuensi yang akan digunakan. Perangkat laptop maupun smartphone umumnya bekerja pada rentang frekuensi 2,4 GHz. Sehingga untuk membangun jaringan wireless pada buku ini, harus dipastikan bahwa yang digunakan adalah rentang frekuensi 2,4 GHz.

Frequency

Rentang frekuensi 2,4 GHz yang digunakan pada implementasi jaringan wireless akan dibagi-bagi menjadi beberapa frekuensi yang sering disebut channel. Untuk negara Indonesia, frekuensi atau channel yang bisa digunakan dapat dilihat pada tabel berikut ini.

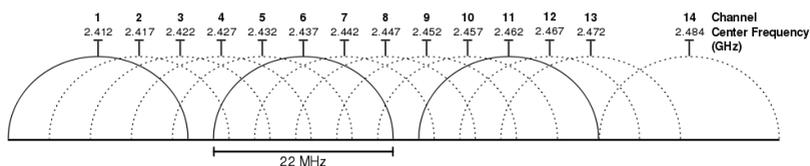
Tabel 5.1
Frekuensi yang dapat digunakan di Indonesia

Channel	Frekuensi (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472

Pada saat mengaktifkan Access Point pada Router MikroTik, Anda harus memilih salah satu frekuensi yang ada pada tabel 5.1. Dan harus dipastikan bahwa frekuensi yang dipilih tersebut berbeda dengan Access Point lain yang kemungkinan berada di sekitar Anda.

Untuk mengetahui ada tidaknya Access Point lain disuatu tempat, beserta berapa frekuensi yang digunakan Access Point lain tersebut, dapat digunakan aplikasi **Wifi Analyzer** pada smartphone Android.

Saat menentukan frekuensi atau channel yang dapat digunakan, sebenarnya terdapat aturan +5/-5. Sebagai contoh, jika di sekitar Anda sudah terdapat jaringan wireless lain yang menggunakan channel 6, maka untuk mencegah interferensi atau gangguan signal, channel yang dapat digunakan adalah channel 11 (6+5) atau bisa memilih channel 1 (6-5). Pemilihan channel dengan aturan tersebut memang ditujukan untuk benar-benar menghindari interferensi antar channel. Ini disebabkan setiap channel memiliki lebar frekuensi yang bisa dilihat pada gambar berikut ini.



Gambar 5.2
Rentang frekuensi 2,4 GHz untuk standar 802.11
(<https://electronics.stackexchange.com>)

SSID

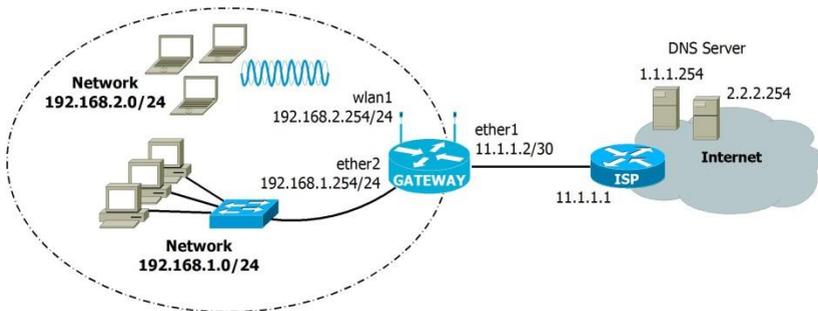
Service Set Identifier (SSID) merupakan identitas atau nama dari sebuah jaringan wireless. SSID inilah yang menjadi panduan bagi pengguna (user) saat menentukan pada jaringan wireless manakah mereka ingin terhubung. SSID dapat dikonfigurasi sepanjang maksimal 32 karakter.

Konfigurasi Dasar

Pada sub bab ini akan dibahas konfigurasi jaringan wireless dengan menggunakan Router MikroTik yang sudah memiliki interface wireless. Secara garis besar, yang harus dilakukan adalah melakukan konfigurasi parameter wireless, konfigurasi IP Address dan mengaktifkan DHCP Server pada interface wireless tersebut. Adapun skenario penerapan jaringan wireless dengan menggunakan router yang tidak memiliki interface wireless akan dibahas pada sub bab selanjutnya.

Topologi

Topologi yang digunakan adalah topologi sederhana, dimana Router MikroTik yang bertugas sebagai Internet Gateway juga bertugas sebagai Access Point. Router untuk skenario seperti ini harus memiliki interface wireless seperti gambar berikut ini.



Gambar 5.3
Router Gateway sebagai Access Point

Dari gambar 5.3, terlihat bahwa Router Gateway memiliki 2 (dua) jaringan lokal, masing-masing adalah jaringan kabel dengan network address 192.168.1.0/24 dan jaringan wireless dengan network address 192.168.2.0/24. Untuk jaringan wireless, interface

yang digunakan adalah interface *wlan1*. Sehingga untuk menjalankan skenario seperti ini, harus dipastikan bahwa router yang digunakan adalah router yang memiliki interface wireless.

Asumsi konfigurasi yang digunakan pada sub bab ini adalah Router MikroTik yang sudah melakukan konfigurasi IP Address pada interface *ether1/ether2*, konfigurasi default route, konfigurasi DNS Server, konfigurasi Firewall masquerade dan konfigurasi DHCP Server pada interface *ether2*. Router Gateway sudah bisa memberikan akses Internet pada komputer yang ada di network 192.168.1.0/24

Konfigurasi Parameter Wireless

Langkah pertama tentunya adalah memastikan bahwa interface *wlan1* sudah diaktifkan. Bila interface *wlan1* masih dalam kondisi disable, maka untuk mengaktifkannya, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > interface set wlan1 disabled=no
```

```
[admin@GATEWAY] > interface print
```

```
Flags: D - dynamic, X - disabled, R - running, S - slave
```

#	NAME	TYPE	AL-MTU	L2MTU	MAX-L2MTU	MAC-ADDR
0	R ether1	ether	1500	1600	4076	D4:CA:6D
1	R ether2	ether	1500	1598	2028	D4:CA:6D
2	X ether3	ether	1500	1598	2028	D4:CA:6D
3	X ether4	ether	1500	1598	2028	D4:CA:6D
4	X ether5	ether	1500	1598	2028	D4:CA:6D
5	wlan1	wlan	1500	1600	2290	D4:CA:6D

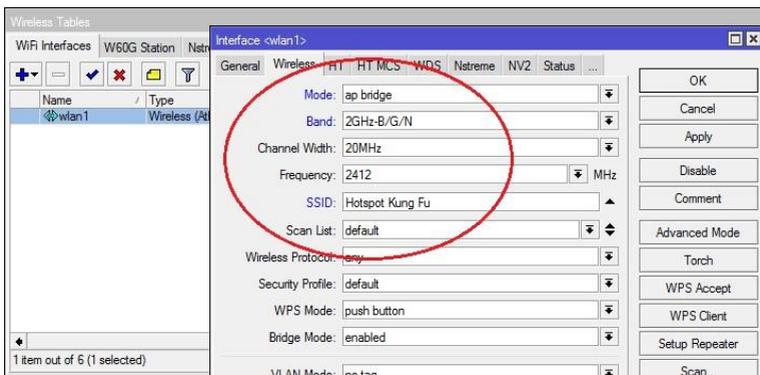
Selanjutnya adalah melakukan konfigurasi parameter wireless pada interface *wlan1*. Untuk skenario ini, tentunya mode yang digunakan haruslah mode *ap-bridge*. Adapun standar yang digunakan adalah 802.11b/g/n dengan frekuensi 2,4 GHz, sehingga parameter band yang digunakan adalah *802.11b/g/n,2GHz*. Adapun frekuensi atau channel yang digunakan adalah channel 1 atau frekuensi 2412 MHz (2,412 GHz) dengan SSID adalah *Hotspot Kung Fu*. Dengan

paramater-parameter tersebut, maka perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > interface wireless set wlan1 mode=ap-bridge \  
band=2ghz-b/g/n frequency=2412 ssid="Hotspot Kung Fu"
```

```
[admin@GATEWAY] > interface wireless print detail  
Flags: X - disabled, R - running  
0 name="wlan1" mtu=1500 l2mtu=1600 mac-  
address=D4:CA:6D:31:4A:D5 arp=enabled interface-  
type=Atheros AR9300 mode=ap-bridge ssid="Hotspot Kung Fu"  
frequency=2412 band=2ghz-b/g/n channel-width=20mhz scan-  
list=default wireless-protocol=any vlan-mode=no-tag vlan-  
id=1 wds-mode=disabled wds-default-bridge=none wds-ignore-  
ssid=no bridge-mode=enabled default-authentication=yes  
default-forwarding=yes default-ap-tx-limit=0 default-  
client-tx-limit=0 hide-ssid=no security-profile=default  
compression=no
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Wireless** → tab **Interfaces**, klik 2x interface → **wlan1**, memilih tab **Wireless**, seperti pada gambar berikut ini.



Gambar 5.4
Parameter wireless pada interface *wlan1*

Setelah konfigurasi di atas dilakukan, pengujian awal yang sederhana dapat dilakukan. Pada kondisi ini, seharusnya signal wireless dari interface *wlan1* akan terlihat pada laptop maupun

smartphone milik user. Namun, jaringan wireless ini belum siap untuk digunakan. Harus dilakukan konfigurasi IP Address maupun DHCP Server pada interface *wlan1* yang akan dibahas pada bagian selanjutnya.

Konfigurasi IP Address

Setelah konfigurasi parameter wireless dilakukan, tahapan selanjutnya adalah memberikan IP Address pada interface *wlan1*. Sesuai skenario, IP Address yang akan diberikan adalah 192.168.2.254/24. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip address add address=192.168.2.254/24 \
interface=wlan1
```

```
[admin@GATEWAY] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK          INTERFACE
0   192.168.1.254/24  192.168.1.0     ether2
1   11.1.1.2/30       11.1.1.0        ether1
2   192.168.2.254/24  192.168.2.0     wlan1
```

Tentunya, dengan menggunakan WinBox, menu yang dapat digunakan adalah menu **IP → Addresses**, tombol **Add**, seperti yang sudah pernah dibahas pada bab sebelumnya.

Langkah terakhir adalah mengaktifkan DHCP Server pada interface *wlan1*. Langkah konfigurasi ini sama dengan konfigurasi saat mengaktifkan DHCP Server pada interface *ether2*. Adapun perintah yang dapat digunakan adalah sebagai berikut.

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

dhcp server interface: wlan1
Select network for DHCP addresses

dhcp address space: 192.168.2.0/24
Select gateway for given network
```

gateway for dhcp network: **192.168.2.254**
Select pool of ip addresses given out by DHCP server

addresses to give out: **192.168.2.1-192.168.2.20**
Select DNS servers

dns servers: **192.168.2.254,1.1.1.254**
Select lease time

lease time: **30m**

Sampai pada tahapan ini, konfigurasi jaringan wireless pada Router Gateway telah selesai dilakukan. Pengujian dapat dilakukan dengan menggunakan laptop maupun smartphone milik user. Dan seharusnya perangkat-perangkat user tersebut akan bisa menikmati layanan Internet.

Pengujian dan Monitoring

Selain pengujian melalui perangkat user, pengujian dan monitoring juga dapat dilakukan melalui Router MikroTik. Pengujian pertama kali dapat dilakukan dengan melihat ada tidaknya label **R (Running)** pada interface *wlan1*. Jika belum terdapat user atau station yang terhubung, maka interface tersebut tidak akan memiliki label **R**. Namun, jika terdapat satu station yang terhubung, maka label **R** akan terlihat pada interface *wlan1*, seperti pada gambar berikut ini.



The screenshot shows the 'Interface List' window in MikroTik WinBox. The 'Interface List' tab is selected, and the 'wlan1' interface is highlighted. The status of 'wlan1' is 'Running', indicated by a green 'R' icon. The table below shows the configuration for various interfaces.

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Fx	Tx F
R	ether1	Ethernet	1500	1600	1120.8 kbps		4.7 Mbps
R	ether2	Ethernet	1500	1598	5.0 Mbps		638.4 kbps
X	ether3	Ethernet	1500	1598	0 bps		0 bps
X	ether4	Ethernet	1500	1598	0 bps		0 bps
X	ether5	Ethernet	1500	1598	0 bps		0 bps
R	wlan1	Wireless (Atheros AR9...	1500	1600	6.6 kbps		3.8 kbps

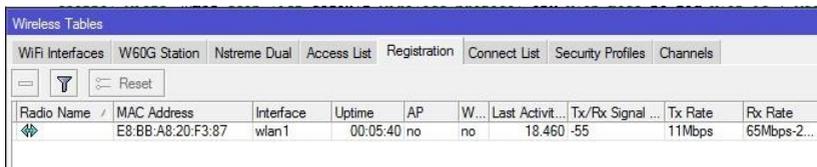
Gambar 5.5
Interface *wlan1* dalam keadaan Running

Selain itu, dapat dilakukan monitoring dengan melihat apakah memang benar ada wireless station yang terhubung ke interface *wlan1* tadi. Jika memang benar ada wireless station yang terhubung, maka MAC Address dari station tersebut akan terlihat pada tabel **Registration** milik interface wireless. Perintah yang dapat digunakan untuk melihat tabel Registration adalah sebagai berikut.

```
[admin@GATEWAY] > interface wireless registration-table print
# INTERFA MAC-ADDRESS      AP  SIGNAL-STRENG TX-RATE UPTIME
0 wlan1    E8:BB:A8:20:F3:87 no   -55dBm@1Mbps  11Mbps  3m4s

[admin@GATEWAY] > interface wireless registration-table \
print detail
0 interface=wlan1 mac-address=E8:BB:A8:20:F3:87 ap=no wds=no
  bridge=no
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Wireless** → tab **Registration**, seperti gambar berikut ini.



The screenshot shows the WinBox interface with the 'Wireless Tables' window open. The 'Registration' tab is selected, displaying a table with the following data:

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
📶	E8:BB:A8:20:F3:87	wlan1	00:05:40	no	no	18.460	-55	11Mbps	65Mbps-2...

Gambar 5.6
Tabel Registration

Dari uraian dan gambar 5.6, terlihat bahwa pada Router MikroTik terdapat 1 (satu) station wireless. Wireless station tersebut adalah perangkat user dengan MAC Address E8:BB:A8:20:F3:87. Terdapat beberapa parameter penting lainnya yang dapat digunakan untuk keperluan monitoring, seperti parameter **Tx-Rate** dan **Rx-Rate** yang menunjukkan bandwidth antara perangkat user dengan interface *wlan1*.

Security Key

Saat diinginkan pengamanan yang lebih baik, maka jaringan wireless bisa saja dilengkapi dengan security key. Fitur security key ini sebenarnya digunakan untuk melakukan pengacakan terhadap data yang dikirimkan antara perangkat wireless user dengan interface *wlan1*. Ini dimaksudkan untuk mencegah penyadapan data yang bisa saja dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

Secara default, Router MikroTik sudah menyediakan satu profil security key yang diberi nama *default*. Untuk melihat profil tersebut dapat menggunakan perintah berikut ini.

```
[admin@GATEWAY] > interface wireless security-profiles print
Flags: * - default
 0 * name="default" mode=none authentication-types="" unicast-
ciphers=aes-ccm group-ciphers=aes-ccm wpa-pre-shared-
key="" wpa2-pre-shared-key="" supplicant-
identity="MikroTik" eap-methods=passthrough tls-mode=no-
certificates tls-certificate=none mschapv2-username=""
mschapv2-password="" static-algo-0=none static-key-0=""
static-algo-1=none static-key-1="" static-algo-2=none
static-key-2="" static-algo-3=none static-key-3=""
static-transmit-key=key-0 static-sta-private-algo=none
static-sta-private-key="" radius-mac-authentication=no
radius-mac-accounting=no radius-eap-accounting=no
interim-update=0s radius-mac-format=XX:XX:XX:XX:XX:XX
radius-mac-mode=as-username radius-mac-caching=disabled
group-key-update=5m management-protection=disabled
management-protection-key=""
```

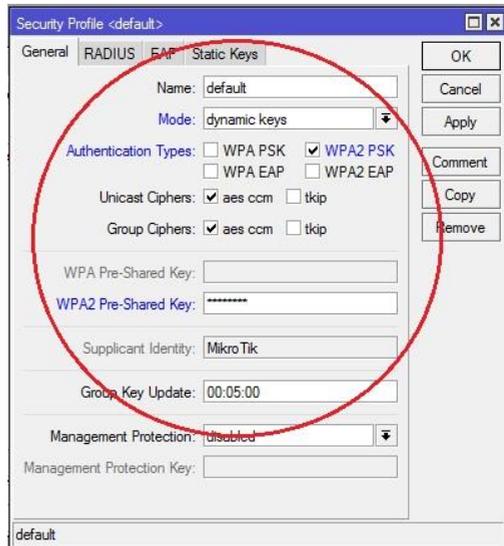
Security key yang disarankan saat ini adalah WPA2, dan untuk mengaktifkannya, Anda harus memasukkan minimal 8 (delapan) karakter yang akan menjadi key. Sebagai contoh, jika key yang digunakan adalah *12345678*, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > interface wireless security-profiles \
set default mode=dynamic-keys authentication-types=wpa2-psk \
wpa2-pre-shared-key=12345678
```

```
[admin@GATEWAY] > interface wireless security-profiles print
Flags: * - default
0 * name="default" mode=dynamic-keys authentication-
types=wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-
ccm wpa-pre-shared-key="" wpa2-pre-shared-key="12345678"
supplicant-identity="MikroTik" eap-methods=passthrough
tls-mode=no-certificates tls-certificate=none mschapv2-
username="" mschapv2-password="" static-algo-0=none
static-key-0="" static-algo-1=none static-key-1=""
static-algo-2=none static-key-2="" static-algo-3=none
static-key-3="" static-transmit-key=key-0 static-sta-
private-algo=none static-sta-private-key="" radius-mac-
authentication=no radius-mac-accounting=no radius-eap-
accounting=no interim-update=0s radius-mac-
format=XX:XX:XX:XX:XX:XX radius-mac-mode=as-username
radius-mac-caching=disabled group-key-update=5m
management-protection=disabled management-protection-
key=""
```

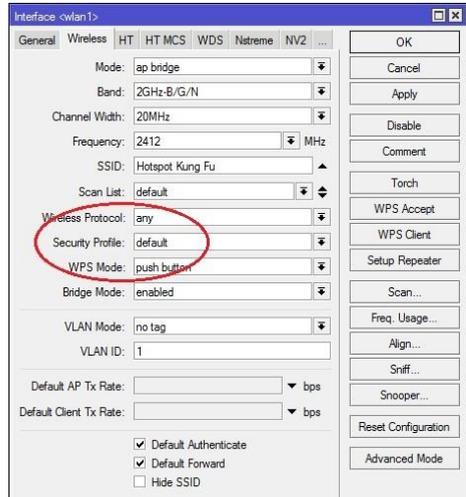
Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Wireless** → tab **Security Profiles**, klik 2x key *default*, memilih tab **General**, seperti gambar berikut ini.

Gambar 5.7
Security key default



Profil *default* ini, juga akan terlihat sebagai parameter *security-profile* pada interface *wlan1*, seperti terlihat pada gambar berikut ini.

Gambar 5.8
Parameter *security-profile* pada
interface *wlan1*

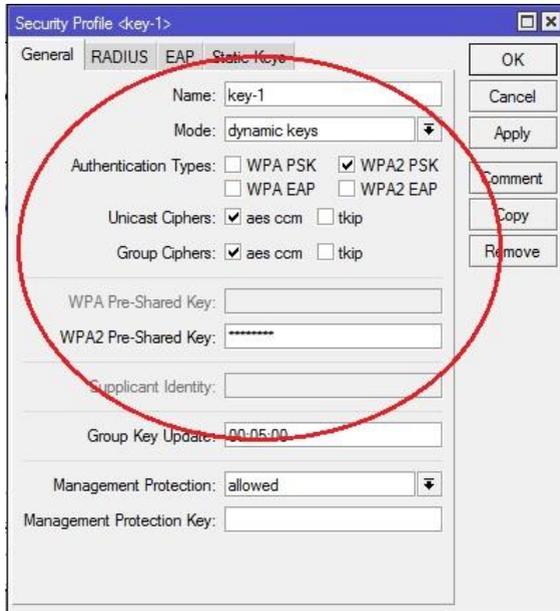


Dengan adanya pilihan parameter *security-profile* pada konfigurasi interface *wlan1*, Anda sebenarnya dapat membuat beberapa pilihan profil security key pada bagian **Security Profiles**, untuk kemudian memilih key-key tersebut pada konfigurasi interface *wlan1*. Mungkin saja Anda menginginkan security key 12345678 pada bulan ini, dan kemudian menggantinya menjadi 87654321 pada bulan depan, dan kemudian membalikannya kembali menjadi 12345678 lagi pada bulan berikutnya lagi 😊.

Sebagai contoh, jika ingin membuat sebuah security key dengan nama *key-1* dan key 87654321, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > interface wireless security-profiles add \
name=key-1 mode=dynamic-keys authentication-types=wpa2-psk \
wpa2-pre-shared-key=87654321
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Wireless** → tab **Security Profiles**, tombol **Add** → tab **General**, seperti pada gambar berikut ini.



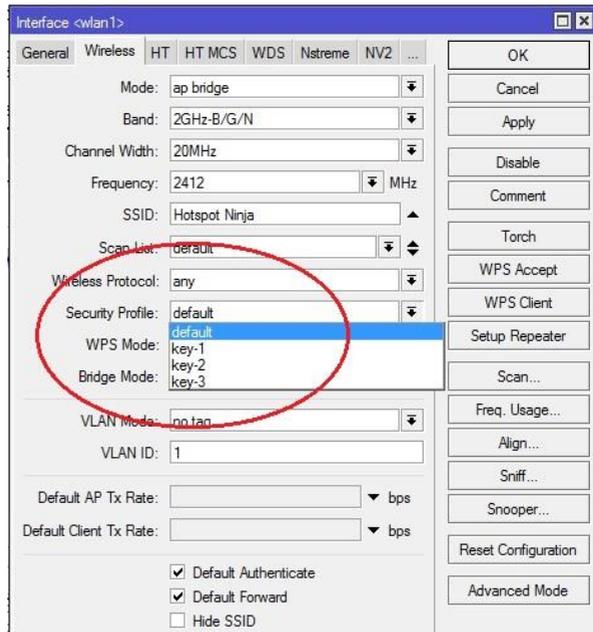
Gambar 5.9
Penambahan Security Key dengan nama *key-1*

Jika Anda telah memiliki beberapa Security Key, maka pada bagian **Security Profiles** akan terlihat seperti gambar berikut ini.

Wireless Tables							
Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels							
Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...	WPA2 Pre-Shared...	
default	dynamic keys	WPA2 PSK	aes ccm	aes ccm	*****	*****	
key-1	dynamic keys	WPA2 PSK	aes ccm	aes ccm	*****	*****	
key-2	dynamic keys	WPA2 PSK	aes ccm	aes ccm	*****	*****	
key-3	dynamic keys	WPA2 PSK	aes ccm	aes ccm	*****	*****	

Gambar 5.10
Beberapa profil security key

Dengan adanya beberapa key pada bagian **Security Profiles**, maka interface *wlan1* akan memiliki beberapa pilihan key, seperti terlihat pada gambar berikut ini.



Gambar 5.11
Interface *wlan1*
memiliki beberapa
pilihan key

Virtual Access Point

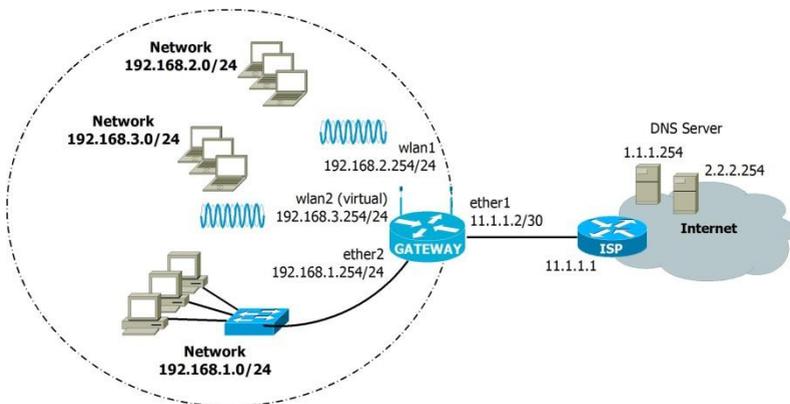
Router MikroTik memiliki fitur Virtual Access Point (Virtual AP) yang dapat digunakan untuk membangun beberapa jaringan wireless, meskipun router yang digunakan hanya memiliki 1 (satu) interface wireless. Beberapa jaringan wireless tersebut akan memiliki SSID beserta IP Address yang berbeda-beda dan security key yang berbeda pula.

Skenario dengan memanfaatkan Virtual AP biasanya diterapkan pada jaringan wireless yang memiliki beberapa karakteristik pengguna (user) yang berbeda. Misalnya saja pada suatu

perusahaan, ingin membedakan antara hotspot karyawan dan hotspot tamu. Dengan Virtual AP, Anda tidak perlu menyediakan banyak interface wireless pada Router MikroTik. Cukup dengan satu interface pada satu router, maka beberapa jaringan wireless tersebut akan mudah untuk dihadirkan.

Topologi

Adapun topologi yang digunakan dapat dilihat pada gambar berikut ini.



Gambar 5.12
Jaringan dengan Virtual AP

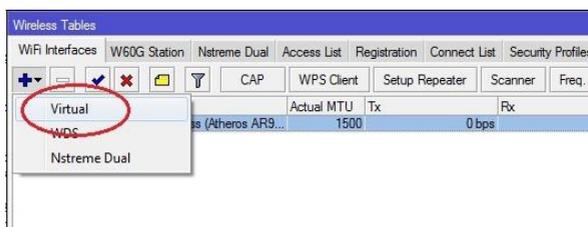
Pada gambar 5.12, terlihat bahwa jaringan wireless yang akan dibangun adalah 2 (dua) jaringan wireless. Kedua jaringan wireless tersebut adalah jaringan 192.168.2.0/24 pada interface *wlan1* dan jaringan 192.168.3.0/24 pada interface *wlan2*. Router MikroTik yang digunakan adalah router dengan 1 (satu) interface wireless, sehingga yang nantinya akan menjadi interface *wlan2* adalah interface virtual.

Asumsi yang digunakan adalah Router MikroTik yang sudah melakukan konfigurasi seperti pada sub bab sebelumnya. Ini berarti Router Gateway sudah melakukan konfigurasi IP Address, default

route, DNS Server, DHCP Server, konfigurasi wireless pada interface *wlan1*. Dengan demikian, pembahasan pada sub bab ini adalah pembahasan khusus untuk konfigurasi penambahan Virtual AP saja.

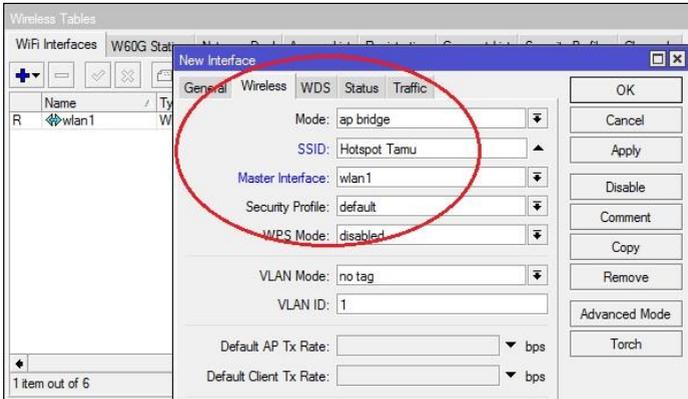
Konfigurasi Virtual Access Point

Untuk menambahkan Virtual Access Point, menu WinBox yang digunakan adalah **Wireless** → tab **Interfaces**, tombol **Add**, memilih **Virtual**, seperti pada gambar berikut ini.



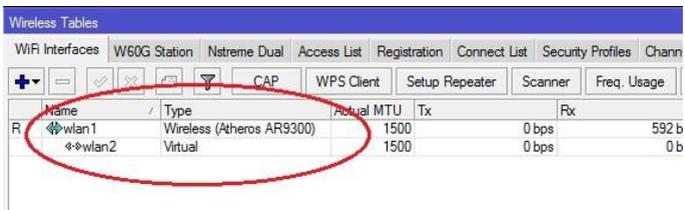
Gambar 5.13
Penambahan Virtual AP

Pada saat menambahkan interface *wlan2*, maka beberapa parameter penting sudah harus dikonfigurasi. Sesuai skenario, parameter wireless yang harus digunakan adalah *mode=ap-bridge* dan *ssid="Hotspot Tamu"*. Adapun parameter *band* maupun *frequency* (channel) tidak bisa dikonfigurasi pada interface virtual. Kedua parameter ini akan mengikuti apa yang sudah digunakan oleh interface *wlan1*. Jadi jika interface *wlan1* sudah menggunakan *frequency* 2,412 GHz, maka otomatis pula interface *wlan2* akan menggunakan frekuensi tersebut.



Gambar 5.14
Interface *wlan2* (virtual)

Setelah melakukan penambahan interface virtual, maka menu **Interfaces** akan terlihat seperti gambar berikut ini.



Gambar 5.15
Interface *wlan1* dan *wlan2*

Dari gambar 5.15, terlihat bahwa interface Virtual AP yang ditambahkan akan diberi nama *wlan2*. Dan terlihat pula bahwa type dari interface tersebut adalah interface virtual yang menginduk pada interface *wlan1*.

Langkah selanjutnya adalah memberikan IP Address 192.168.3.254/24 pada interface *wlan2* dengan menggunakan perintah berikut ini.

```
[admin@GATEWAY] > ip address add address=192.168.3.254/24 \
interface=wlan2
```

```
[admin@GATEWAY] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK    INTERFACE
0   192.168.1.254/24   192.168.1.0   ether2
1   11.1.1.2/30        11.1.1.0     ether1
2   192.168.2.254/24   192.168.2.0   wlan1
3   192.168.3.254/24   192.168.3.0   wlan2
```

Selanjutnya adalah konfigurasi DHCP Server pada interface *wlan2* dengan menggunakan perintah berikut ini.

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

dhcp server interface: wlan2
Select network for DHCP addresses

dhcp address space: 192.168.3.0/24
Select gateway for given network

gateway for dhcp network: 192.168.3.254
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.3.1-192.168.3.20
Select DNS servers

dns servers: 192.168.3.254,1.1.1.254
Select lease time

lease time: 30m
```

Sampai pada tahapan ini, semua konfigurasi pada interface *wlan2* telah selesai. Namun, yang perlu diperhatikan adalah parameter *security-profile* pada interface *wlan2*. Pada konfigurasi ini terlihat bahwa *security-profile* yang digunakan adalah profil *default* yang ternyata sama dengan yang digunakan oleh interface *wlan1*. Kondisi

ini dapat dilihat seperti uraian berikut ini, perhatikanlah parameter *security-profile=default*.

```
[admin@GATEWAY] > interface wireless print
Flags: X - disabled, R - running
0  name="wlan1" mtu=1500 l2mtu=1600 mac-
    address=D4:CA:6D:31:4A:D5 arp=enabled interface-
    type=Atheros AR9300 mode=ap-bridge ssid="Hotspot Kung Fu"
    frequency=2412 band=2ghz-b/g/n channel-width=20mhz scan-
    list=default wireless-protocol=any vlan-mode=no-tag vlan-
    id=1 wds-mode=disabled wds-default-bridge=none wds-ignore-
    ssid=no bridge-mode=enabled default-authentication=yes
    default-forwarding=yes default-ap-tx-limit=0 default-
    client-tx-limit=0 hide-ssid=no security-profile=default
    compression=no

1  name="wlan2" mtu=1500 l2mtu=1600 mac-
    address=D6:CA:6D:31:4A:D5 arp=enabled interface-
    type=virtual master-interface=wlan1 mode=ap-bridge
    ssid="Hotspot Tamu" vlan-mode=no-tag vlan-id=1 wds-
    mode=disabled wds-default-bridge=none wds-ignore-ssid=no
    bridge-mode=enabled default-authentication=yes default-
    forwarding=yes default-ap-tx-limit=0 default-client-tx-
    limit=0 hide-ssid=no security-profile=default
```

Umumnya, jaringan wireless yang berbeda akan menggunakan proteksi keamanan yang berbeda pula. Sehingga pekerjaan yang masih harus dilakukan adalah membedakan security key antara interface *wlan1* dan *wlan2*.

Security Key

Pada bagian ini akan dikonfigurasi security key yang berbeda antara interface *wlan1* dan *wlan2*. Sesuai skenario, jaringan wireless Hotspot Tamu tidak akan menggunakan security key. Adapun langkah pertama yang harus dilakukan adalah membuat profile tanpa key. Parameter yang digunakan pada profile ini adalah *mode=none*. Jika profil ini akan diberi nama *tanpa-key*, maka perintah yang dapat digunakan adalah sebagai berikut.

```

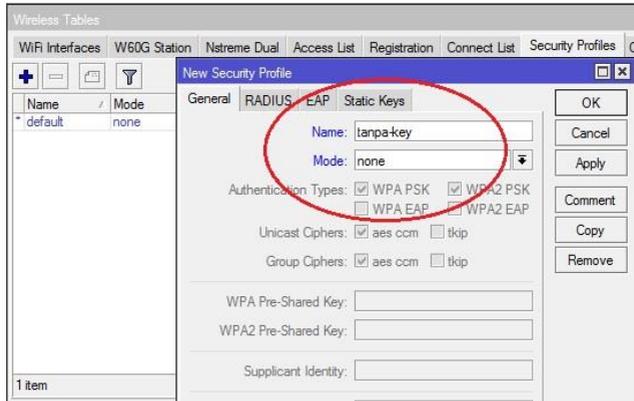
[admin@GATEWAY] > interface wireless security-profiles add \
name=tanpa-key mode=none

[admin@GATEWAY] > interface wireless security-profiles print
Flags: * - default
0 * name="default" mode=dynamic-keys authentication-
types=wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-
ccm wpa-pre-shared-key="" wpa2-pre-shared-key="12345678"
supplicant-identity="MikroTik" eap-methods=passthrough
tls-mode=no-certificates tls-certificate=none mschapv2-
username="" mschapv2-password="" static-algo-0=none
static-key-0="" static-algo-1=none static-key-1=""
static-algo-2=none static-key-2="" static-algo-3=none
static-key-3="" static-transmit-key=key-0 static-sta-
private-algo=none static-sta-private-key="" radius-mac-
authentication=no radius-mac-accounting=no radius-eap-
accounting=no interim-update=0s radius-mac-
format=XX:XX:XX:XX:XX:XX radius-mac-mode=as-username
radius-mac-caching=disabled group-key-update=5m
management-protection=disabled management-protection-
key=""

1 name="tanpa-key" mode=none authentication-types=""
unicast-ciphers=aes-ccm group-ciphers=aes-ccm wpa-pre-
shared-key="" wpa2-pre-shared-key="" supplicant-
identity="Gateway" eap-methods=passthrough tls-mode=no-
certificates tls-certificate=none mschapv2-username=""
mschapv2-password="" static-algo-0=none static-key-0=""
static-algo-1=none static-key-1="" static-algo-2=none
static-key-2="" static-algo-3=none static-key-3=""
static-transmit-key=key-0 static-sta-private-algo=none
static-sta-private-key="" radius-mac-authentication=no
radius-mac-accounting=no radius-eap-accounting=no
interim-update=0s radius-mac-format=XX:XX:XX:XX:XX:XX
radius-mac-mode=as-username radius-mac-caching=disabled
group-key-update=5m management-protection=disabled
management-protection-key=""

```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Wireless** → tab **Security Profiles**, tombol **Add** → tab **General**, seperti pada gambar berikut ini



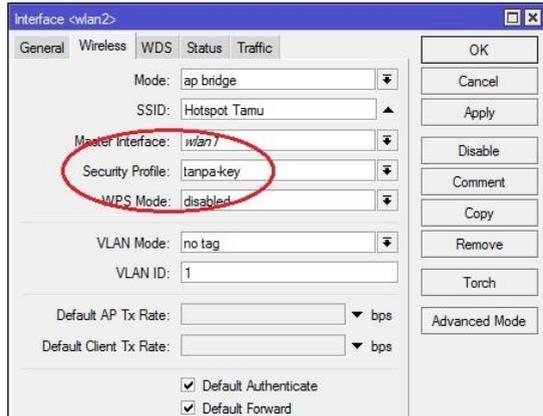
Gambar 5.16
Security Profile tanpa key

Langkah terakhir adalah menggunakan profile *tanpa-key* tadi sebagai parameter *security-profiles* pada interface *wlan2*. Adapun perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > interface wireless set wlan2
security-profile=tanpa-key

[admin@GATEWAY] > interface wireless print
Flags: X - disabled, R - running
0 name="wlan1" mtu=1500 l2mtu=1600 mac-address=D4:CA:6D:31:4A:D5 arp=enabled interface-type=Atheros AR9300 mode=ap-bridge ssid="Hotspot Kungfu" frequency=2412 band=2ghz-b/g/n channel-width=20mhz scan-list=default wireless-protocol=any vlan-mode=no-tag vlan-id=1 wds-mode=disabled wds-default-bridge=none wds-ignore-ssid=no bridge-mode=enabled default-authentication=yes default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0 hide-ssid=no security-profile=default compression=no
1 name="wlan2" mtu=1500 l2mtu=1600 mac-address=D6:CA:6D:31:4A:D5 arp=enabled interface-type=virtual master-interface=wlan1 mode=ap-bridge ssid="Hotspot Tamu" vlan-mode=no-tag vlan-id=1 wds-mode=disabled wds-default-bridge=none wds-ignore-ssid=no bridge-mode=enabled default-authentication=yes default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0 hide-ssid=no security-profile=tanpa-key
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Wireless** → tab **Interfaces**, klik 2x interface *wlan2*, kemudian memilih tab **Wireless**, seperti pada gambar berikut ini.



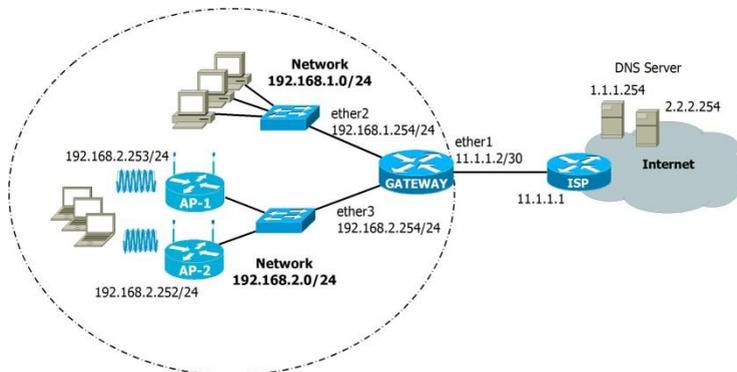
Gambar 5.17
Profile *tanpa-key* pada
interface *wlan2*

Perluasan Jaringan Wireless

Pada beberapa kondisi, akses jaringan wireless yang akan diberikan meliputi area kerja yang relatif luas. Sehingga untuk penerapan di lapangan membutuhkan beberapa unit Access Point. Untuk skenario seperti ini umumnya Router MikroTik yang digunakan sebagai Internet Gateway adalah router yang tidak memiliki interface wireless. Sehingga dibutuhkan konfigurasi yang saling mendukung antara router yang bertugas sebagai Internet Gateway dengan router yang bertugas sebagai Access Point. Terkadang pula router yang bertugas sebagai Access Point menggunakan perangkat dari vendor lain. Namun, karena buku ini adalah buku MikroTik, maka contoh pembahasan akan menggunakan Access Point dari Router MikroTik.

Topologi

Adapun topologi yang digunakan adalah satu unit Router MikroTik sebagai Internet Gateway dan 2 (dua) unit Router MikroTik sebagai Access Point. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 5.18
Jaringan dengan 2 (dua) Access Point

Pada gambar 5.18, jaringan wireless yang akan dibangun adalah jaringan 192.168.2.0/24. Jumlah Access Point yang digunakan adalah 2 (dua) Access Point, masing-masing adalah AP-1 dan AP-2. Kedua Access Point tersebut akan menggunakan IP Address 192.168.2.253 untuk AP-1 dan 192.168.2.252 untuk AP-2. Adapun Router Gateway adalah Router MikroTik yang tidak memiliki interface wireless. Kedua Access Point akan dihubungkan ke interface *ether3* dari Router Gateway dan IP Address pada interface *ether3* tersebut adalah 192.168.2.254.

Konfigurasi Internet Gateway

Asumsi yang digunakan adalah Router Gateway yang sudah melakukan konfigurasi IP Address pada interface *ether1* dan *ether2*, melakukan konfigurasi default route, konfigurasi DNS Server,

konfigurasi Firewall Masquerade dan DHCP Server pada interface *ether2*. Konfigurasi tersebut sudah dibahas pada bab-bab sebelumnya.

Sehingga untuk mewujudkan skenario seperti pada gambar 5.18, Router Gateway hanya perlu melakukan penambahan IP Address pada interface *ether3* sekaligus mengaktifkan DHCP server pada interface *ether3* tersebut. Adapun konfigurasi-konfigurasi parameter wireless akan dilakukan pada Access Point AP-1 dan AP-2. Bukankah Router Gateway merupakan router tanpa interface wireless, sehingga menu wireless sekalipun akan tidak terlihat pada router ini.

Adapun perintah penambahan IP Address, dapat dilakukan dengan perintah berikut ini.

```
[admin@GATEWAY] > ip address add address=192.168.2.254/24 \
interface=ether3
```

Untuk mengaktifkan DHCP Server, perintah yang dapat digunakan adalah sebagai berikut.

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

dhcp server interface: ether3
Select network for DHCP addresses

dhcp address space: 192.168.2.0/24
Select gateway for given network

gateway for dhcp network: 192.168.2.254
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.2.1-192.168.2.30
Select DNS servers

dns servers: 192.168.2.254,1.1.1.254
Select lease time

lease time: 30m
```

Konfigurasi Access Point

Router MikroTik yang mendukung untuk menjadi Access Point pada skenario ini tentu adalah Router MikroTik yang memiliki minimal 1 (satu) interface wireless dan minimal 1 (satu) interface kabel. Contoh perangkat yang bisa digunakan adalah Router MikroTik RBcAP2nD, seperti terlihat pada gambar berikut ini.



Gambar 5.19
RouterBoard seri RBcAP2nD

Pada AP-1 konfigurasi wireless dapat dilakukan pada interface *wlan1* dengan menggunakan perintah berikut ini.

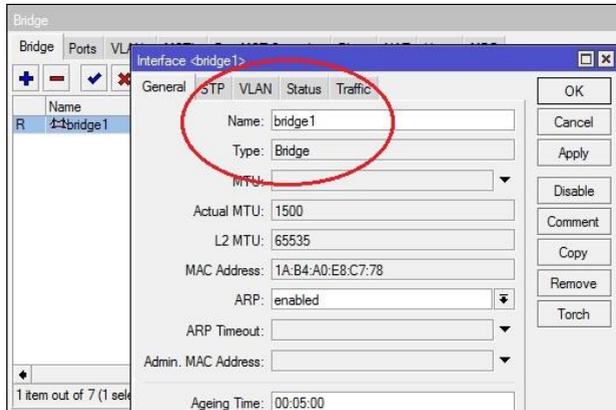
```
[admin@AP-1] > interface wireless set wlan1 mode=ap-bridge \  
band=2ghz-b/g/n frequency=2412 ssid="Hotspot Kung Fu"
```

Selanjutnya adalah melakukan konfigurasi bridge atau konfigurasi yang bisa menjembatani antara interface *wlan1* dan *ether1*. Adapun perintah yang dapat dilakukan adalah membuat interface bridge terlebih dahulu dengan menggunakan perintah berikut ini.

```
[admin@AP-1] > interface bridge add name=bridge1
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Bridge** → tab **Bridge**, tombol **Add** → tab **General**, seperti pada gambar berikut ini.

Gambar 5.20
Membuat
interface bridge

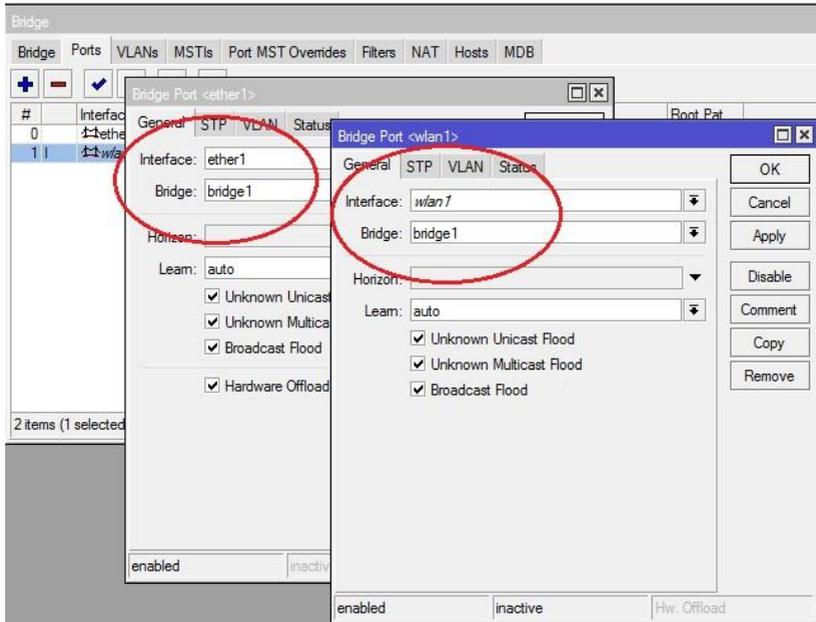


Selanjutnya adalah memasukkan interface *ether1* dan *wlan1* ke dalam interface *bridge1* tadi. Adapun perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@AP-1] > interface bridge port add interface=ether1 \  
bridge=bridge1
```

```
[admin@AP-1] > interface bridge port add interface=wlan1 \  
bridge=bridge1
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah menu **Bridge** → tab **Port**, tombol **Add** seperti gambar berikut ini. Perlu diperhatikan bahwa Anda harus menambahkan interface *ether1* dan *wlan1* ke dalam interface *bridge1*.



Gambar 5.21

Memasukkan interface *ether1* dan *wlan1* ke dalam *bridge1*

Langkah terakhir adalah menambahkan IP Address pada interface *bridge1*, sekaligus memberikan konfigurasi default route. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@AP-1] > ip address add address=192.168.2.253/24 \
interface=bridge1
```

```
[admin@AP-1] > ip route add gateway=192.168.2.254
```

Untuk AP-2, langkah konfigurasi bisa dikatakan relatif sama. Konfigurasi parameter wireless pada AP-2 dapat menggunakan perintah berikut ini.

```
[admin@AP-2] > interface wireless set wlan1 mode=ap-bridge \
band=2ghz-b/g/n frequency=2437 ssid="Hotspot Kung Fu"
```

Konfigurasi bridge dapat menggunakan perintah berikut ini.

```
[admin@AP-2] > interface bridge add name=bridge1

[admin@AP-2] > interface bridge port add interface=ether1 \
bridge=bridge1

[admin@AP-2] > interface bridge port add interface=wlan1 \
bridge=bridge1

[admin@AP-2] > ip address add address=192.168.2.252/24 \
interface=bridge1

[admin@AP-2] > ip route add gateway=192.168.2.254
```

Sampai pada tahapan ini, semua konfigurasi jaringan wireless baik pada Router Gateway yang bertugas sebagai Internet Gateway dan DHCP Server, maupun Router AP-1 dan AP-2 sebagai Access Point telah selesai dilakukan. Seharusnya perangkat wireless milik user akan mudah terhubung ke Internet baik menggunakan AP-1 maupun AP-2. Dan perangkat wireless tersebut seharusnya akan menggunakan IP Address dari network 192.168.2.0/24.

Sebagai catatan, pada konfigurasi Access Point di atas, sedikit telah menggunakan teknik bridge. Teknik bridge ini adalah teknik yang menghubungkan beberapa interface yang ada didalam satu router. Teknik bridge ini akan dibahas lebih mendalam pada buku **MikroTik Kung Fu Kitab 2, terbitan Jasakom**.

Monitoring

Monitoring dengan topologi seperti pada gambar 5.18 akan sedikit berbeda dengan topologi sebelumnya. Namun sebenarnya memiliki konsep monitoring yang sama.

Untuk melihat jumlah user wireless yang terhubung ke jaringan berdasarkan IP Address yang didapatkan dari DHCP Server, maka

Anda harus melihat tabel **Leases** pada DHCP Server yang ada di Router Gateway. Seperti terlihat pada gambar berikut ini.

Address	MAC Address	Client ID	Server	Active Address	Active MAC Address
192.168.1.1	08:00:27:05:1F:DC	1:d0:67:e5:11:d:56	all		
D 192.168.1.2	D0:67:E5:11:0D:56	1:d0:67:e5:11:d:56	dhcp1	192.168.1.2	D0:67:E5:11:0D:56
192.168.1.3	08:00:27:29:4B:F7	1:8:0:27:29:4b:f7	dhcp1		
D 192.168.2.20	30:CB:F8:CC:D5:8F	1:30:cb:f8:cc:d5:8f	dhcp2	192.168.2.20	30:CB:F8:CC:D5:8F
D 192.168.2.19	E8:BB:A8:20:F3:87		dhcp2	192.168.2.19	E8:BB:A8:20:F3:87

Gambar 5.22
IP Address dari user wireless pada DHCP Server

Dari uraian di atas terlihat ada 2 (dua) user wireless yang terhubung, masing-masing dengan IP Address 192.168.2.20 dan 192.168.2.19. Dengan hanya melihat uraian ini, Anda belum bisa melihat pada Access Point manakah kedua user terhubung.

Untuk melihat pada Access Point mana sebuah user atau station wireless terhubung, maka yang harus diperhatikan adalah tabel **Registration** pada masing-masing Access Point. Sebagai contoh, gambar berikut memperlihatkan bahwa user wireless dengan MAC Address 30:CB:F8:CC:D5:8F terhubung pada AP-1.

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activ...	Tx/Rx Signal ...	Tx Rate	Rx Rate
	30:CB:F8:CC:D5:8F	wlan1	02:07:58	no	no	0.190 -56	72.2Mbps...	65Mbps-2...	

Gambar 5.23
Tabel Registration pada AP-1

Sedangkan station atau user wireless dengan MAC Address E8:BB:A8:20:F3:87, terhubung pada AP-2, seperti yang diperlihatkan gambar berikut yang merupakan tabel **Registration** dari AP-2.



Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
	E8:BB:A8:20:F3:87	wlan1	01:17:39	no	no	3.030	-42	72.2Mbps...	65Mbps-2...

Gambar 5.24
Tabel Registration pada AP-2

End of Chapter

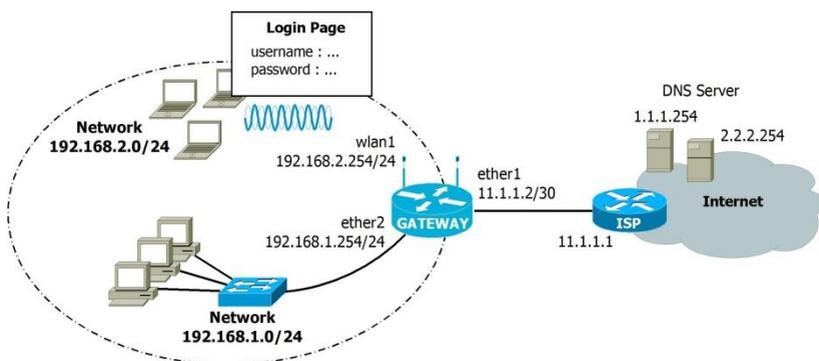
Bab 06

Hotspot Server

Melakukan manajemen terhadap pengguna jaringan terkadang merupakan pekerjaan yang tidak mudah. Apalagi yang akan dikendalikan adalah pengguna jaringan wireless. Untuk membatasi penggunaan akses wireless, pada bab sebelumnya sudah diberikan konfigurasi dengan menggunakan security key. Namun, penggunaan security saja tidaklah mampu untuk melakukan manajemen secara menyeluruh. Bukankah hanya tersedia satu key yang nantinya akan digunakan oleh beberapa user secara bersamaan. Bagaimana jika ada user yang memberikan key tersebut ke orang lain yang sebenarnya tidak berhak menggunakan akses jaringan wireless Anda.

Untuk menjawab tantangan tadi, Router MikroTik menyediakan sebuah fitur yang diberi nama Hotspot Server. Dengan Hotspot Server, setiap pengguna jaringan akan diberikan username dan password masing-masing, berbeda antara user yang satu dengan user yang lain. Saat akan mengakses Internet, maka seorang user akan dihadapkan dengan halaman web login. Pada halaman login

inilah username dan password tersebut harus digunakan jika user yang bersangkutan akan mengakses Internet.



Gambar 6.1
Penerapan Hotspot Server

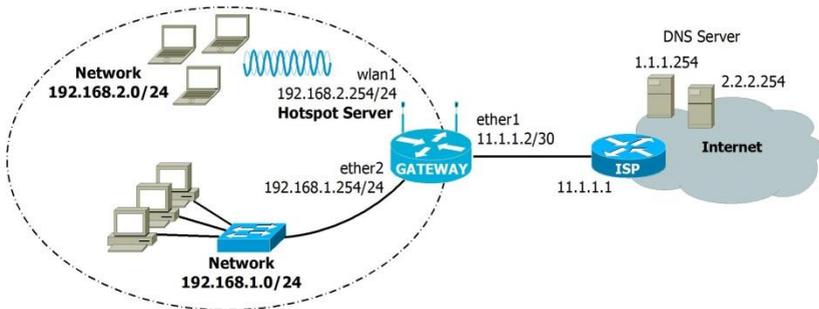
Selain itu, masih banyak fitur yang dimiliki oleh Hotspot Server, seperti berapa lama sebuah account username dapat digunakan, berapa batasan kuota download maupun upload dari user tersebut, website apa saja yang bisa diakses oleh seorang user, dan masih banyak lagi fitur-fitur yang akan memudahkan pekerjaan pengelolaan jaringan.

Walaupun bernama Hotspot Server, fitur ini bisa saja diterapkan pada jaringan kabel. Dengan kata lain, fitur ini bisa diaktifkan pada interface *wlan* maupun diaktifkan pada interface *ether*.

Pada buku ini hanya akan dibahas konfigurasi dasar dari Hotspot Server. Walaupun demikian, konfigurasi yang dibahas sudah dapat digunakan untuk mengelola jaringan sederhana yang memerlukan perhatian khusus dalam hal pengelolaan user.

Konfigurasi Dasar

Sebelum melakukan konfigurasi Hotspot Server, maka harus dipastikan terlebih dahulu topologi yang akan digunakan. Dari topologi inilah akan bisa ditentukan pada interface mana Hotspot Server akan diaktifkan. Adapun topologi yang akan digunakan pada bab ini dapat dilihat pada gambar berikut ini.



Gambar 6.2
Hotspot Server diaktifkan pada *wlan1*

Dari gambar 6.2, terlihat bahwa Router Gateway langsung melayani jaringan wireless dengan menggunakan interface *wlan1*. Jaringan tersebut menggunakan network address 192.168.2.0/24. Dari skenario ini, diinginkan bahwa Hotspot Server akan diaktifkan pada interface *wlan1*. Meskipun demikian, Hotspot Server juga bisa diaktifkan pada interface *ether2*, barangkali Anda ingin juga melakukan manajemen user pada pengguna jaringan kabel.

Asumsi awal yang digunakan pada sub bab ini adalah Router Gateway sudah melakukan konfigurasi IP Address pada interface *ether1/ether2*, sudah melakukan konfigurasi default route, konfigurasi DNS Server, konfigurasi Firewall Masquerade, dan sudah mengaktifkan DHCP Server pada interface *ether2*. Parameter wireless pada interface *wlan1* seperti *mode*, *band*, *frequency* dan *ssid*,

juga sudah dikonfigurasi seperti pembahasan pada bab sebelumnya. Untuk skenario ini, security key tidak diterapkan pada interface *wlan1*. Adapun IP Address pada interface *wlan1* juga belum dikonfigurasi.

Untuk melakukan konfigurasi Hotspot Server, langkah pertama adalah memberikan IP Address pada interface *wlan1*. IP Address yang akan digunakan adalah 192.168.2.254/24, perintah yang digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip address add address=192.168.2.254/24 \
interface=wlan1
```

Jika ingin mengaktifkan Hotspot Server pada sebuah interface, maka konfigurasi DHCP Server tidak diperlukan. Ini karena instalasi Hotspot Server akan secara otomatis mengaktifkan DHCP Server.

Selanjutnya adalah mengaktifkan Hotspot Server dengan menggunakan pilihan *Hotspot Setup*. Pada saat mengaktifkan Hotspot Server, nantinya akan dikonfigurasi parameter-parameter seperti berikut ini.

- *hotspot interface*, parameter yang menunjukkan pada interface mana Hotspot Server akan diaktifkan. Pada skenario ini akan dipilih interface *wlan1*.
- *local address of network*, parameter yang menunjukkan gateway yang akan digunakan pada jaringan Hotspot Server. Umumnya adalah IP Address dari interface di mana Hotspot Server diaktifkan. Pada skenario ini tentunya adalah 192.168.2.254/24.
- *masquerade network*, jika jaringan yang digunakan adalah jaringan lokal yang terhubung langsung ke Internet, maka parameter ini harus menggunakan pilihan *yes*.
- *address pool of network*, parameter ini menunjukkan range atau rentang IP Address yang akan dibagi-bagikan kepada perangkat user. Parameter ini sama dengan parameter *address-pool* pada DHCP Server. Untuk skenario ini, akan digunakan rentang IP

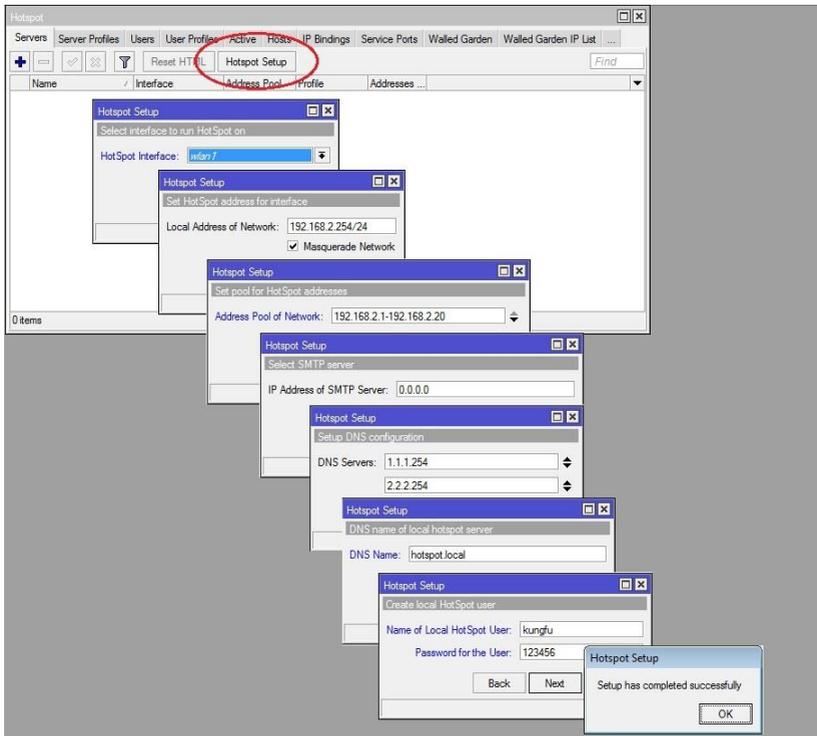
Address 192.168.2.1 s/d 192.168.2.20, ini berarti ada sekitar 20 user yang dapat menggunakan Hotspot Server secara bersamaan.

- *select certificate*, parameter ini menunjukkan ada tidaknya sertifikat SSL yang akan digunakan. Pada skenario ini tidak ada sertifikat SSL yang akan digunakan, sehingga pilihan yang diambil adalah *no*.
- *ip address of smtp server*, parameter ini menunjukkan ada tidaknya SMTP Server yang digunakan. Pada skenario ini, akan digunakan pilihan *0.0.0.0* yang menunjukkan bahwa tidak ada SMTP Server yang akan digunakan.
- *dns servers*, parameter ini menunjukkan konfigurasi DNS Server yang akan diberikan kepada perangkat user. Umumnya disesuaikan dengan DNS Server pada jaringan tersebut maupun konfigurasi DNS dari ISP. Untuk skenario ini akan digunakan DNS server 1.1.1.254 dan 2.2.2.254.
- *dns name*, parameter ini menunjukkan domain dari Hotspot Server yang digunakan. User akan diarahkan pada alamat domain ini pada saat akan mengakses Internet. Dengan mengakses domain tersebut, juga akan bisa ditampilkan halaman login atau status dari Hotspot Server. Untuk skenario ini, domain yang akan digunakan adalah *hotspot.local*.
- *name of local hotspot user* dan *password for the user*, parameter ini menunjukkan username pertama (berserta password) yang dapat digunakan untuk menguji Hotspot Server. Sebagai contoh, username yang akan digunakan adalah *kungfu* dengan password *123456*.

Setelah mengetahui kegunaan dari parameter-parameter yang akan digunakan, maka langkah selanjutnya adalah mengaktifkan Hotspot Server dengan perintah sebagai berikut.

```
[admin@GATEWAY] > ip hotspot setup  
Select interface to run HotSpot on  
  
hotspot interface: wlan1  
Set HotSpot address for interface  
  
local address of network: 192.168.2.254/24  
masquerade network: yes  
Set pool for HotSpot addresses  
  
address pool of network: 192.168.2.1-192.168.2.20  
Select hotspot SSL certificate  
  
select certificate: none  
Select SMTP server  
  
ip address of smtp server: 0.0.0.0  
Setup DNS configuration  
  
dns servers: 1.1.1.254,2.2.2.254  
DNS name of local hotspot server  
  
dns name: hotspot.local  
Create local hotspot user  
  
name of local hotspot user: kungfu  
password for the user: 123456
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Hotspot → tab Server**, tombol **Hotspot Setup**, seperti pada gambar berikut ini.



Gambar 6.3
Hotspot Setup

Setelah konfigurasi seperti pada Gambar 6.3, maka Hotspot Server telah selesai diaktifkan, dan dapat dilihat dengan menggunakan perintah berikut ini.

```
[admin@GATEWAY] > ip hotspot print detail
Flags: X - disabled, I - invalid, S - HTTPS
0 name="hotspot1" interface=wlan1 address-pool=hs-pool-1
  profile=hsprof1 idle-timeout=5m keepalive-timeout=none
  login-timeout=none addresses-per-mac=2 ip-of-dns-
  name=192.168.2.254 proxy-status="running"
```

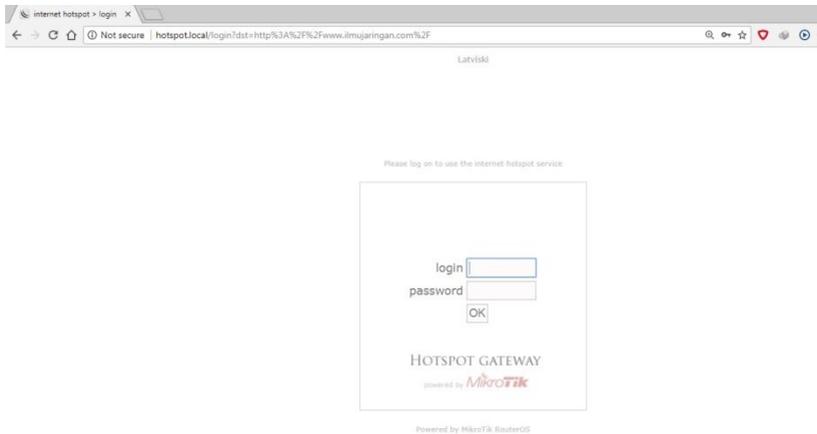
Dengan menggunakan WinBox, Hotspot Server ini dapat dilihat pada menu **IP → Hotspot → tab Server**, seperti pada gambar berikut ini.



Gambar 6.4
Hotspot Server dengan nama hotspot1

Sampai pada tahapan ini, instalasi Hotspot Server sudah selesai dan terlihat bahwa Hotspot Server yang berhasil diaktifkan diberi nama *hotspot1*. Hotspot Server ini sudah siap digunakan, dan untuk melakukan pengujian awal, Anda bisa menghubungkan laptop ke jaringan wireless di *wlan1* dan mencoba membuka sebuah website dengan browser. Karena Hotspot Server tidak menggunakan sertifikat SSL, maka halaman yang pertama kali dibuka sebaiknya adalah web site dengan protokol HTTP.

Sebagai contoh, jika laptop user pada jaringan Hotspot Server mencoba membuka web site *www.detik.com*, maka akan terlihat halaman login seperti berikut ini.



Gambar 6.5
Halaman Login

Dari gambar 6.5, terlihat bahwa user yang ingin mengakses Internet akan berhadapan dengan halaman login terlebih dahulu. Jika ingin mendapatkan akses Internet, user tersebut harus memasukkan username *kungfu* dengan password *123456*.

Adapun konfigurasi penambahan username akan dibahas pada sub bab selanjutnya.

Manajemen User

Untuk dapat digunakan oleh banyak user, maka harus dilakukan penambahan account pada sistem Hotspot Server. Masing-masing account tersebut akan langsung dapat dibatasi waktu penggunaannya, quota upload, quota download maupun gabungan antara quota download dan upload (quota total).

Menambahkan user

Sebagai contoh, untuk menambahkan account untuk user *alundra* dengan password *qwerty*, maka perintah yang dapat digunakan adalah sebagai berikut.

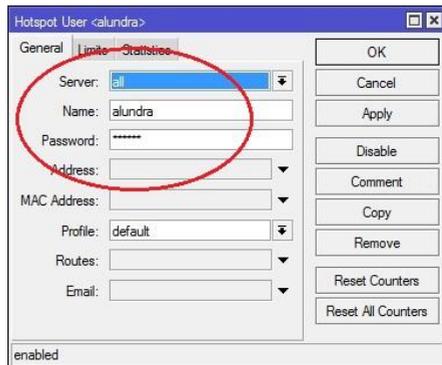
```
[admin@GATEWAY] > ip hotspot user add name=alundra \
password=qwerty
```

```
[admin@GATEWAY] > ip hotspot user print detail
Flags: * - default, X - disabled, D - dynamic
0 * ;;; counters and limits for trial users
  name="default-trial" uptime=0s bytes-in=0 bytes-out=0
  packets-in=0 packets-out=0

1  name="kungfu" password="123456" profile=default uptime=0s
  bytes-in=0 bytes-out=0 packets-in=0 packets-out=0

2  name="alundra" password="qwerty" profile=default uptime=0s
  bytes-in=0 bytes-out=0 packets-in=0 packets-out=0
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Hotspot → tab Users**, tombol **Add → tab General** seperti pada gambar berikut ini.



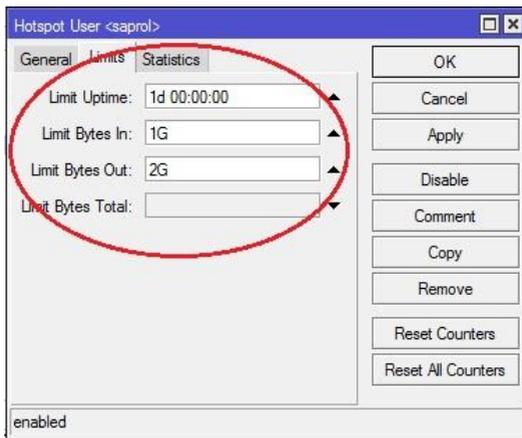
Gambar 6.6
Menambahkan user *alundra*

Jika ingin menambahkan user *saprol*, namun account ini akan dibatasi pemakaiannya selama 24 jam, dengan batasan kuota upload

sebesar 1 GB dan download 2 GB, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip hotspot user add name=saprol \
password=654321 limit-uptime=24:00:00 limit-bytes-out=2G \
limit-bytes-in=1G
```

Dengan menggunakan WinBox, parameter *uptime*, quota download (*byte-out*) dan quota upload (*byte-in*) dapat dikonfigurasi pada tab **Limits**, seperti pada gambar berikut ini.



Gambar 6.7
Limitasi untuk user *saprol*

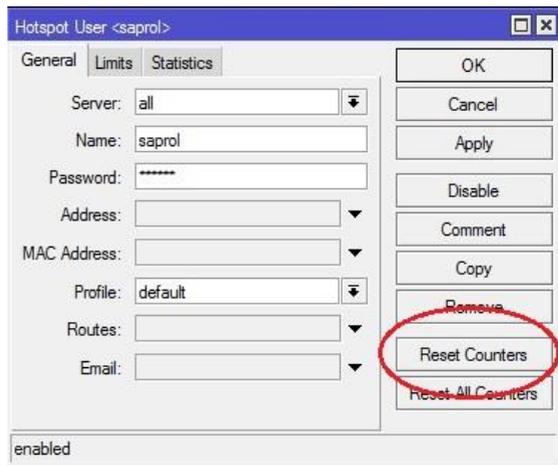
Untuk user *saprol*, limitasi apa saja yang akan tercapai terlebih dahulu akan membuat username tersebut tidak dapat digunakan lagi. Misalnya saja, user *saprol* baru menggunakan account-nya selama 1 jam, namun sudah melakukan download sebesar 2 GB, maka account user *saprol* akan dinonaktifkan (tidak dapat digunakan lagi), meskipun belum digunakan selama 24 jam.

Jika sebuah account user sudah mencapai limitasi-nya, agar user account tersebut dapat kembali digunakan, harus dilakukan *reset counter*. Misalnya, user *saprol* sudah mencapai limitasi-nya, untuk

mengembalikan user tersebut sehingga dapat digunakan kembali, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip hotspot user reset-counters saprol
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Hotspot → tab Users**, meng-klik 2x user *saprol*, kemudian memilih tombol **Reset Counters**, seperti pada gambar berikut ini.



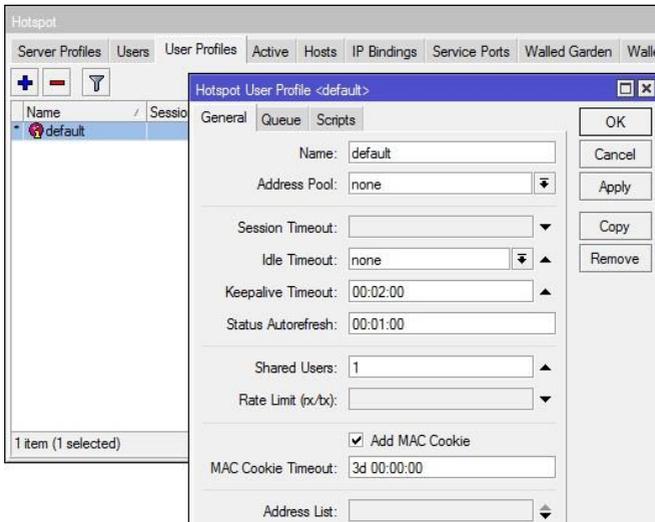
Gambar 6.8
Reset Counters untuk
user saprol

Mengenal User Profile

Setiap user akan dimasukkan ke dalam sebuah profil user, dan secara default profil user yang akan diberikan adalah profil *default*. Profil ini dapat dilihat dengan menggunakan perintah berikut ini.

```
[admin@GATEWAY] > ip hotspot user profile print detail
Flags: * - default
0 * name="default" idle-timeout=none keepalive-timeout=2m
  status-autorefresh=1m shared-users=1 add-mac-cookie=yes
  mac-cookie-timeout=3d address-list="" transparent-
  proxy=no
```

Dengan menggunakan WinBox, profil user dapat dilihat dengan menggunakan menu **IP → Hotspot → tab User Profiles**, klik 2x profil *default*, seperti terlihat pada gambar berikut ini.



Gambar 6.9
Profil user *default*

Pada profil user terdapat berbagai parameter yang juga akan menentukan fasilitas apa saja yang akan diberikan kepada user yang menggunakan profil ini. Sebagai contoh, pada profil *default* ini terdapat parameter *shared-user=1*. Dan, jika melihat contoh penambahan user sebelumnya, user *kungfu*, *alundra* dan *saprol* akan menggunakan profil *default* ini. Dengan demikian, user account *kungfu* hanya akan bisa digunakan secara bersamaan pada satu perangkat saja. Begitu pula dengan user *alundra* dan *saprol*, masing-masing hanya bisa digunakan pada satu perangkat secara bersamaan. Ini karena ketiga user tersebut menggunakan profil user *default*, dan parameter *shared-user* pada profil *default* bernilai 1.

Untuk melakukan manajemen user yang lebih mendalam, Anda bisa saja melakukan penambahan profil user dan memasukkan user tertentu pada profil tersebut. Sebagai contoh, jika diinginkan ada profil *publik* dengan parameter *shared-user=40*, maka perintah yang dapat digunakan adalah sebagai berikut.

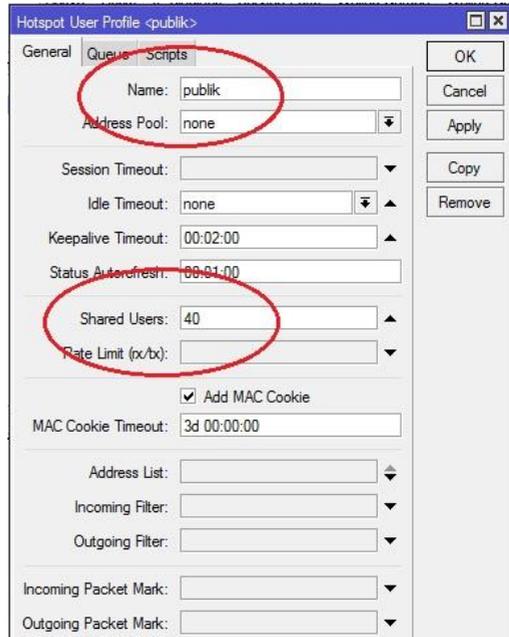
```
[admin@GATEWAY] > ip hotspot user profile add \
name=publik shared-users=40

[admin@GATEWAY] > ip hotspot user profile print detail
Flags: * - default
0 * name="default" idle-timeout=none keepalive-timeout=2m
  status-autorefresh=1m shared-users=1 add-mac-cookie=yes
  mac-cookie-timeout=3d address-list="" transparent-
  proxy=no

1 name="publik" idle-timeout=none keepalive-timeout=2m
  status-autorefresh=1m shared-users=40 add-mac-cookie=yes
  mac-cookie-timeout=3d address-list="" transparent-
  proxy=no
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Hotspot → tab User Profiles**, tombol **Add → tab General**, seperti pada gambar berikut ini.

Gambar 6.10
Penambahan profil *publik*



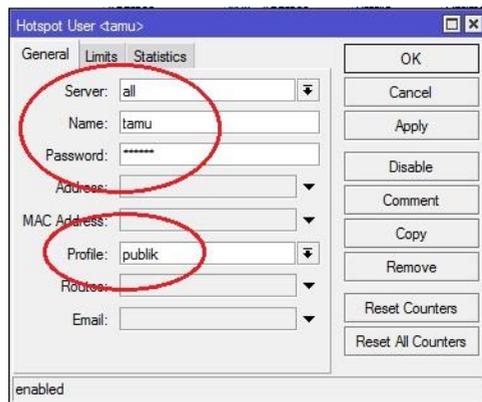
Kemudian, jika diinginkan ada sebuah username yang bisa digunakan oleh 40 perangkat secara bersamaan, maka username tersebut dapat menggunakan profil *publik* tadi. Perintah berikut ini adalah perintah untuk membuat username *tamu*, dimana username *tamu* akan menggunakan profil *publik*, sehingga nantinya username *tamu* dapat digunakan oleh 40 perangkat secara bersamaan.

```
[admin@GATEWAY] > ip hotspot user add name=tamu
password=123456 profile=publik
```

```
[admin@GATEWAY] > ip hotspot user print detail
Flags: * - default, X - disabled, D - dynamic
0 * ;;; counters and limits for trial users
name="default-trial" uptime=0s bytes-in=0 bytes-out=0
packets-in=0 packets-out=0
```

- 1 name="kungfu" password="123456" profile=default uptime=0s bytes-in=0 bytes-out=0 packets-in=0 packets-out=0
- 2 name="alundra" password="qwerty" profile=default uptime=0s bytes-in=0 bytes-out=0 packets-in=0 packets-out=0
- 3 name="saprol" password="654321" profile=default limit-uptime=1d limit-bytes-in=1000000000 limit-bytes-out=2000000000 uptime=0s bytes-in=0 bytes-out=0 packets-in=0 packets-out=0
- 4 name="tamu" password="123456" profile=publik uptime=0s bytes-in=0 bytes-out=0 packets-in=0 packets-out=0

Dengan menggunakan WinBox, maka menu yang dapat digunakan adalah IP → Hotspot → tab Users, tombol Add → tab General, seperti pada gambar berikut ini.



Gambar 6.11
Penambahan user tamu

Monitoring

Untuk melakukan monitoring pada jaringan yang sudah menggunakan Hotspot Server, Anda harus mengetahui terlebih dahulu prosedur seorang user saat akan berhadapan dengan Hotspot Server di suatu jaringan. Bila suatu jaringan sudah

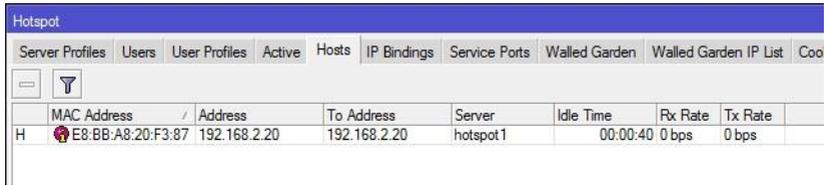
mengaktifkan Hotspot Server, maka tahapan user untuk mendapatkan akses Internet dapat dijabarkan sebagai berikut.

1. Yang paling pertama terjadi adalah user terhubung ke jaringan wireless yang menggunakan Hotspot Server. Atau bisa juga terhubung ke jaringan kabel yang juga mengaktifkan Hotspot Server. Pada kondisi ini, tidak ada satu pun layanan Internet yang akan didapatkan oleh user tersebut.
2. Jika user ingin menggunakan layanan Internet, user tersebut harus membuka web browser untuk mengakses halaman login. Pada halaman login inilah, user akan bisa mengisikan username dan password yang dimilikinya.
3. Untuk mengakses halaman login, user bisa saja mengetikkan alamat Hotspot Server. Alamat Hotspot Server adalah alamat yang Anda isikan pada parameter *dns-name* saat mengaktifkan Hotspot Server. Pada skenario ini, alamatnya adalah *hotspot.local*. Selain itu, user bisa langsung membuka alamat web site yang dituju, misalnya *www.detik.com*. Hotspot Server mempunyai kemampuan untuk mengarahkan user ke halaman login tadi.
4. Setelah halaman login terbuka, user harus memasukkan username dan password yang berlaku (valid). Jika username dan password tersebut diterima oleh sistem Hotspot Server, maka user akan mendapatkan akses Internet.

Dari tahapan proses penggunaan Hotspot Server di atas, saat user terhubung ke jaringan wireless (atau pun kabel) yang memiliki Hotspot Server, maka MAC Address dari perangkat yang digunakan user akan terlihat pada tabel **Host**. Untuk melihat tabel **Host**, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > ip hotspot host print
Flags: S - static, H - DHCP, D - dynamic, A - authorized, P - bypassed
#   MAC-ADDRESS      ADDRESS      TO-ADDRESS  SERVER
0 H E8:BB:A8:20:F3:87 192.168.2.20 192.168.2.20 hotspot1
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Hotspot → tab Hosts**, seperti pada gambar berikut ini.



	MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate	
H	E8:BB:A8:20:F3:87	192.168.2.20	192.168.2.20	hotspot1	00:00:40	0 bps	0 bps	

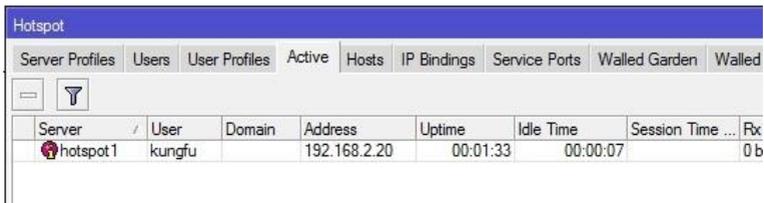
Gambar 6.12
Tabel Host.

Pada uraian dan Gambar 6.11, terlihat bahwa perangkat dengan MAC Address E8:BB:A8:20:F3:87 telah terhubung pada Hotspot Server. Juga terlihat bahwa perangkat tersebut belum melakukan authentication, atau belum memasukkan username dan password. Meskipun demikian, perangkat tersebut sudah mendapatkan IP Address, terlihat bahwa perangkat tersebut sudah menggunakan IP Address 192.168.2.20. Pada kondisi ini, Anda akan dapat melihat kehadiran perangkat ini pada tabel Leases milik DHCP Server.

Jika suatu saat user tersebut sudah melakukan authentication atau sudah memasukkan username dan password yang benar, maka username atau account yang digunakannya akan terlihat pada tabel **Active**, tentu saja MAC Addressnya masih saja terlihat di tabel **Host**. Untuk melihat tabel **Active**, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > ip hotspot active print detail
Flags: R - radius, B - blocked
0 server=hotspot1 user="kungfu" address=192.168.2.20 mac-
address=E8:BB:A8:20:F3:87 login-by="http-chap" uptime=12s
keepalive-timeout=2m
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Hotspot → tab Active**, seperti pada gambar berikut ini.



Server	User	Domain	Address	Uptime	Idle Time	Session Time ...	Rx
hotspot1	kungfu		192.168.2.20	00:01:33	00:00:07		0 b

Gambar 6.13
Tabel Active

Halaman Login

Pada saat user pertama kali mengakses Internet, maka halaman login yang akan ditemui oleh user tersebut akan terlihat seperti pada Gambar 6.5. Halaman login tersebut disusun dari beberapa file berekstensi html, yang memang merupakan bahasa standar dalam pemrograman web. File-file penyusun halaman web tersebut akan disimpan dalam sebuah folder atau direktori yang bernama *hotspot*. Direktori tersebut akan disimpan pada disk Router MikroTik, dan dapat dilihat dengan menggunakan perintah berikut ini.

```
[admin@GATEWAY] > file print
# NAME                                TYPE                                SIZE CREATION-TIME
0 hotspot/alogin.html                 .html file                         1307 dec/21/2017 14:
1 hotspot/error.html                 .html file                         898  dec/21/2017 14:
2 hotspot/errors.txt                  .txt file                          3615 dec/21/2017 14:
3 hotspot/favicon.ico                 .ico file                          903  dec/21/2017 14:
4 hotspot/img/logobotto               .png file                          3925 dec/21/2017 14:
5 hotspot/login.html                 .html file                         3455 dec/21/2017 14:
6 hotspot/logout.html                .html file                         1813 dec/21/2017 14:
7 hotspot/lv                          directory                          dec/21/2017 14:
8 hotspot/lv/alogin.htm               .html file                         1303 dec/21/2017 14:
9 hotspot/lv/errors.txt               .txt file                          3810 dec/21/2017 14:
10 hotspot/lv/login.html              .html file                         3408 dec/21/2017 14:
11 hotspot/lv/radvert.ht              .html file                         1475 dec/21/2017 14:
12 hotspot/lv/status.htm              .html file                         2760 dec/21/2017 14:
13 hotspot/radvert.html               .html file                         1509 dec/21/2017 14:
14 hotspot/rlogin.html                .html file                         850  dec/21/2017 14:
15 hotspot/status.html                .html file                         3009 dec/21/2017 14:
```

```

16 hotspot/xml                directory          dec/21/2017 14:
17 hotspot/xml/WISPAcces .xsd file          4251 dec/21/2017 14:

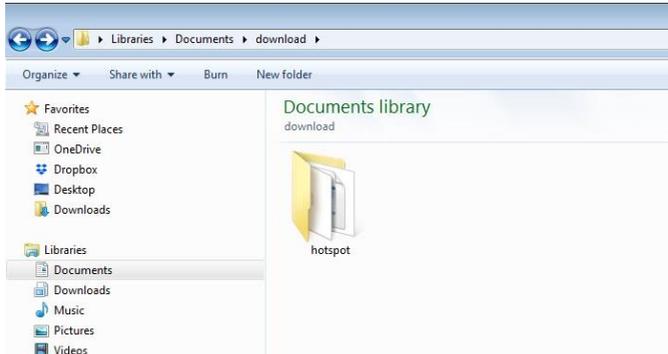
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah menu **Files**, seperti terlihat pada gambar berikut ini.

File Name	Type	Size	Creation Time
auto-before-reset.backup	backup	14.4 KB	Dec/19/2017 05:22:38
hotspot	directory		Dec/21/2017 14:00:56
hotspot/alogin.html	html file	1307 B	Dec/21/2017 14:00:56
hotspot/error.html	html file	898 B	Dec/21/2017 14:00:56
hotspot/errors.txt	txt file	3615 B	Dec/21/2017 14:00:56
hotspot/favicon.ico	ico file	903 B	Dec/21/2017 14:00:56
hotspot/img	directory		Dec/21/2017 14:00:56
hotspot/img/logobottom.png	png file	3925 B	Dec/21/2017 14:00:56
hotspot/login.html	html file	3455 B	Dec/21/2017 14:00:56
hotspot/logout.html	html file	1813 B	Dec/21/2017 14:00:56
hotspot/iv	directory		Dec/21/2017 14:00:56
hotspot/iv/alogin.html	html file	1303 B	Dec/21/2017 14:00:56
hotspot/iv/errors.txt	txt file	3810 B	Dec/21/2017 14:00:56
hotspot/iv/login.html	html file	3408 B	Dec/21/2017 14:00:56
hotspot/iv/logout.html	html file	1843 B	Dec/21/2017 14:00:56
hotspot/iv/radvert.html	html file	1475 B	Dec/21/2017 14:00:56
hotspot/iv/status.html	html file	2760 B	Dec/21/2017 14:00:56
hotspot/md5.js	js file	7.0 KB	Dec/21/2017 14:00:56
hotspot/radvert.html	html file	1509 B	Dec/21/2017 14:00:56
hotspot/redirect.html	html file	318 B	Dec/21/2017 14:00:56
hotspot/rogin.html	html file	850 B	Dec/21/2017 14:00:56
hotspot/status.html	html file	3009 B	Dec/21/2017 14:00:56
hotspot/xml	directory		Dec/21/2017 14:00:56
hotspot/xml/WISPAccessGa...	xsd file	4251 B	Dec/21/2017 14:00:56
hotspot/xml/alogin.html	html file	821 B	Dec/21/2017 14:00:56
hotspot/xml/error.html	html file	416 B	Dec/21/2017 14:00:56
hotspot/xml/flogout.html	html file	361 B	Dec/21/2017 14:00:56

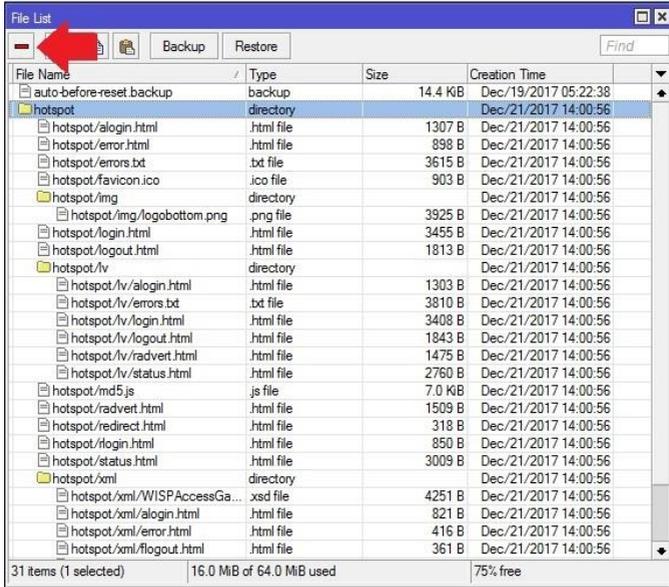
Gambar 6.14
Direktori *hotspot* tempat penyimpanan halaman login

Untuk melakukan perubahan tampilan dari halaman login, Anda bisa saja mengganti file-file tersebut dengan template halaman login yang banyak tersedia di Internet. Template yang tersedia di Internet juga umumnya akan disimpan pada direktori hotspot. Gambar berikut ini memperlihatkan template yang sudah di-download dari alamat <http://mikrotikthemes.airpoint.club/2015/02/digital-ocean.html>



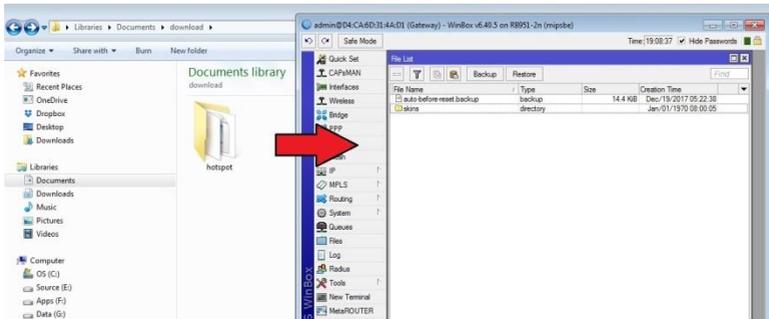
Gambar 6.15
Template halaman login

Jika template halaman login yang baru sudah tersedia, maka direktori *hotspot* yang ada di dalam Router MikroTik dapat dihapus. Prosedur menghapus direktori tersebut dapat dilakukan dengan menggunakan menu **Files**, memilih direktori *hotspot*, dan menghapusnya dengan menggunakan tombol **Remove**, seperti pada gambar berikut ini.



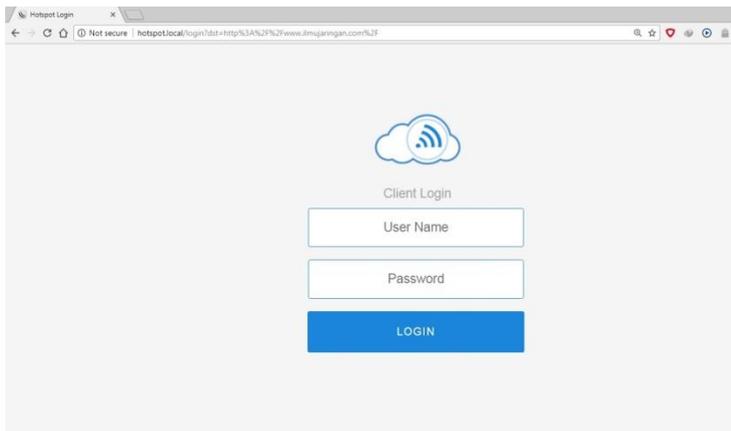
Gambar 6.16
Menghapus halaman login

Jika halaman login sudah dihapus, maka Anda tinggal memindahkan template yang sudah di-download tadi ke dalam menu **Files** pada Router MikroTik. Untuk memindahkannya, dapat menggunakan prosedur *drag n drop*, menggeser direktori *hotspot* dari komputer Anda ke dalam menu **Files**, seperti pada gambar berikut ini.



Gambar 6.17
Memindahkan halaman login

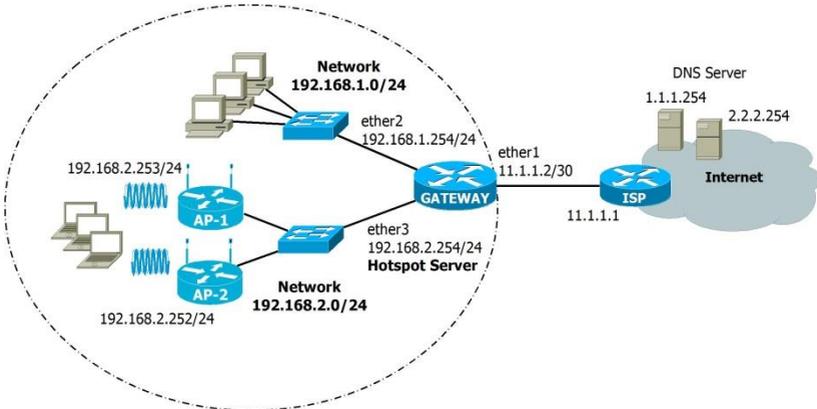
Setelah halaman login yang baru ditempatkan pada menu **Files**, maka tampilan dari halaman login akan berganti, seperti pada gambar berikut ini.



Gambar 6.18
Halaman login yang sudah dimodifikasi

Skenario Lain

Untuk skenario topologi jaringan dengan Router MikroTik yang tidak memiliki interface wireless, maka Hotspot Server akan diaktifkan pada interface ether. Topologinya dapat dilihat seperti pada gambar berikut ini.



Gambar 6.19
Jaringan wireless dengan 2 (dua) Access Point

Topologi di atas adalah contoh topologi yang pernah dibahas pada Bab Wireless sebelumnya. Pada kondisi seperti ini, harus dipastikan bahwa Access Point AP-1 dan AP-2 yang digunakan harus berada dalam kondisi bridge. Konfigurasi bridge tersebut juga sudah dibahas pada Bab Wireless sebelumnya. Adapun Hotspot Server harus diaktifkan pada interface *ether3* Router Gateway, dengan langkah-langkah konfigurasi yang sama seperti Anda mengaktifkannya pada interface *wlan1* sebelumnya.

End of Chapter

Bab 07

Bandwidth Management

Setelah melakukan konfigurasi pada pembahasan bab sebelumnya, Anda sebenarnya sudah bisa menghubungkan jaringan lokal ke Internet. User atau pengguna yang ada di jaringan lokal seharusnya sudah bisa mendapatkan layanan Internet. Bahkan pada Bab Hotspot Server, Anda sudah bisa melakukan manajemen user, sehingga bisa mengatur user mana saja yang bisa mendapatkan akses Internet.

Yang menjadi pertanyaan selanjutnya adalah bagaimana memberikan jaminan kualitas layanan Internet yang diberikan kepada masing-masing user. Faktor yang paling menentukan dalam memberikan jaminan layanan Internet yang baik adalah cukup tidaknya bandwidth yang bisa diberikan kepada setiap user. Semakin besar bandwidth yang diberikan maka akan semakin baik layanan Internet yang diberikan. Namun, jika bandwidth yang tersedia relatif tidak banyak, maka sangat penting untuk

memberikan pengaturan besaran bandwidth yang bisa didapatkan oleh masing-masing user.

Untuk memberikan jaminan bandwidth yang realistis (atau yang masuk akal) kepada tiap-tiap user, maka langkah selanjutnya adalah menerapkan Quality of Service (QoS).

Tindakan yang bisa diambil saat akan menjalankan QoS adalah melakukan manajemen bandwidth. Dengan manajemen bandwidth, Anda sebagai pengelola jaringan dituntut untuk memberikan alokasi bandwidth yang realistis kepada setiap user. Tentunya alokasi yang realistis tersebut adalah alokasi bandwidth yang masuk akal saat akan menggunakan Internet. Jangan sampai Anda memberikan alokasi bandwidth yang sangat kecil (tidak masuk akal) sehingga layanan Internet yang diberikan menjadi kurang nyaman ☺.

Konsep Dasar Manajemen Bandwidth

Traffic yang dikirimkan baik ke Internet maupun dari Internet akan terdiri dari potongan-potongan paket data, lebih tepatnya lagi IP Packet atau sering disebut packet saja ☺. Semakin besar bandwidth yang diberikan oleh ISP, maka akan semakin banyak paket yang bisa dikirimkan dalam rentang waktu tertentu. Dan untuk mengatur bandwidth yang nantinya akan diberikan kepada setiap user, maka harus dilakukan pengaturan paket.

Melakukan manajemen bandwidth sebenarnya melakukan pengaturan antrian terhadap paket-paket yang akan diberikan kepada setiap user. Dengan kata lain, ilmu manajemen bandwidth adalah ilmu antrian paket, atau ilmu antrian (ilmu queue). Ada banyak teknik-teknik antrian yang dapat digunakan, antara lain :

- FIFO (First In First Out)
- Priority Queuing
- CBQ (Class Based Queuing)

- RED (Random Early Drop)
- SFQ (Stochastic Fairness Queuing)
- HTB (Hierarchical Token Bucket (HTB))
- PCQ (Per Connection Queuing)
- dan lain-lain

Untuk pembahasan buku ini, teori antrian tidak akan dibahas. Pembahasan pada buku ini akan cenderung kepada implementasi atau penerapan, sehingga yang dibahas adalah konfigurasi manajemen bandwidth. Teori dan konsep yang mendalam tentang ilmu manajemen bandwidth atau ilmu queue akan dibahas pada Buku **MikroTik Kung Fu Kitab 3**, terbitan **Jasakom**.

CIR dan MIR

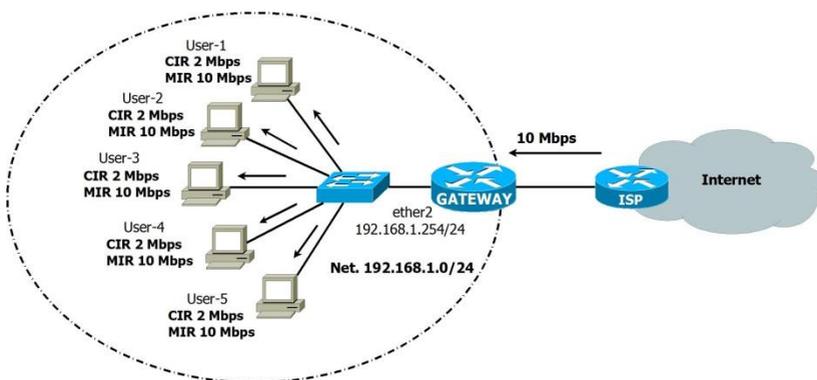
Saat memberikan jaminan bandwidth kepada user atau pengguna Internet dikenal 2 (dua) batasan atau rate, yaitu :

- **Committed Information Rate (CIR)**, batasan ini merupakan alokasi bandwidth paling rendah yang bisa didapatkan oleh seorang user. Seorang user akan mendapatkan nilai CIR-nya saat kondisi jaringan sangat sibuk, saat semua user yang ada di jaringan tersebut menggunakan semua alokasi bandwidth-nya. Pada saat penerapan manajemen bandwidth, Anda harus bisa menentukan nilai CIR yang akan diberikan.
- **Maximum Information Rate (MIR)**, batasan ini adalah alokasi bandwidth paling tinggi yang bisa didapatkan seorang user. Nilai MIR akan bisa didapatkan seorang user jika dalam jaringan tersebut tidak ada user lain yang sedang menggunakan alokasi bandwidthnya masing-masing.

Dari uraian konsep CIR dan MIR, bisa didapatkan kesimpulan besar bahwa nilai MIR akan didapatkan seorang user, jika kondisi jaringan sedang sepi. Sedangkan, jika jaringan berada dalam kondisi teramat sibuk, atau berada dalam kondisi terburuk, maka user tersebut akan

mendapatkan nilai CIR-nya. Kondisi lain yang bisa terjadi adalah jaringan tidak terlalu sibuk atau tidak terlalu sepi, maka seorang user mungkin akan mendapatkan alokasi bandwidth antara nilai CIR dan nilai MIR-nya.

Sebagai contoh jika sebuah jaringan memiliki alokasi bandwidth download sebesar 10 Mbps, dan jaringan tersebut berisi 5 (lima) komputer, maka skenario pembagian nilai CIR dan MIR-nya dapat dilihat pada ilustrasi berikut ini.



Gambar 7.1

Jaringan dengan alokasi 10 Mbps untuk download

Dari gambar 7.1, terlihat bahwa alokasi bandwidth 10 Mbps dari ISP akan dibagi rata ke semua komputer yang ada di jaringan tersebut. Jika ternyata pada jaringan tersebut hanya komputer *user-1* yang menggunakan alokasi bandwidth, maka komputer tersebut bisa mendapatkan semua alokasi bandwidth sebesar 10 Mbps. Dengan kata lain, komputer *user-1* berhasil mendapatkan nilai MIR-nya.

Masih dari gambar 7.1, bagaimana jika semua komputer menggunakan alokasi bandwidth-nya. Jika kondisi ini terjadi, maka alokasi 10 Mbps tersebut akan dibagi rata ke seluruh komputer. Dan masing-masing komputer (termasuk komputer *user-1*) akan

mendapatkan alokasi 2 Mbps. Dengan kata lain, semua komputer user hanya mendapatkan nilai CIR-nya.

Bagaimana jika pada jaringan tersebut yang menggunakan alokasi bandwidth hanya komputer *user-1* dan *user-2*. Karena hanya ada 2 (dua) komputer yang menggunakan alokasi bandwidth, maka alokasi 10 Mbps akan dibagi rata, masing-masing 5 Mbps untuk *user-1* dan *user-2*. Dengan kata lain, pada kondisi yang tidak terlalu sibuk, maka *user-1* akan mendapatkan alokasi bandwidth di antara nilai CIR dan MIR-nya, begitu pula dengan alokasi bandwidth yang diterima oleh *user-2*.

Queue pada Router MikroTik

Router MikroTik memiliki 2 (dua) fitur utama untuk menjalankan manajemen bandwidth. Kedua fitur tersebut adalah sebagai berikut.

- **Simple Queue**, fitur ini dapat digunakan untuk melakukan pengaturan bandwidth sederhana, dan merupakan cara termudah untuk membagi-bagi bandwidth. Namun, untuk jaringan dengan skenario pembagian bandwidth yang rumit, penerapan Simple Queue justru akan membuat konfigurasi menjadi lebih rumit.
- **Queue Tree**, fitur ini umumnya digunakan pada jaringan yang menuntut skenario pembagian bandwidth yang lebih rumit. Penerapan Queue Tree membutuhkan konfigurasi Firewall Mangle terlebih dahulu. Sehingga, jika Anda ingin menggunakan Queue Tree, maka kemampuan melakukan konfigurasi Firewall Mangle yang baik merupakan sesuatu yang tidak bisa ditawar lagi 😊.

Pembahasan konfigurasi manajemen bandwidth pada buku ini akan menggunakan Simple Queue. Untuk kebutuhan jaringan dengan skala kecil maupun menengah, penggunaan Simple Queue

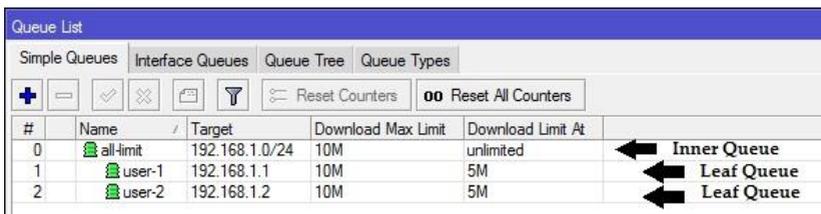
sebenarnya sudah sangat cukup. Adapun Penggunaan Queue Tree akan dibahas pada buku **MikroTik Kung Fu Kitab 2**.

Inner Queue dan Leaf Queue

Konfigurasi Simple Queue maupun Queue Tree dapat dibuat berhirarki atau bersusun. Pada susunan queue hirarki akan terdapat 2 (dua) jenis queue, masing-masing adalah sebagai berikut.

- **Inner Queue**, queue ini bertugas untuk melakukan distribusi bandwidth kepada konfigurasi queue yang lain. Sehingga inner queue terlihat hanya sebagai pembagi bandwidth kepada sejumlah komputer di dalam jaringan. Inner queue juga dapat melakukan distribusi bandwidth kepada beberapa jaringan, jika terdapat beberapa jaringan lokal (multiple network). Inner Queue sering disebut sebagai parent atau queue induk.
- **Leaf Queue**, queue ini bertugas untuk memberikan alokasi bandwidth kepada komputer user. Leaf queue setidaknya akan menginduk ke sebuah Inner Queue. Sebagai catatan, terkadang Leaf Queue juga bertugas memberikan alokasi bandwidth kepada sebuah jaringan. Namun yang perlu diingat, Leaf Queue tidak lagi memiliki queue lain yang menginduk kepadanya.

Contoh ilustrasi queue yang telah disusun dengan konsep hirarki dapat dilihat pada gambar berikut ini.



#	Name	Target	Download Max Limit	Download Limit At	
0	all-limit	192.168.1.0/24	10M	unlimited	← Inner Queue
1	user-1	192.168.1.1	10M	5M	← Leaf Queue
2	user-2	192.168.1.2	10M	5M	← Leaf Queue

Gambar 7.2
Simple Queue yang berhirarki

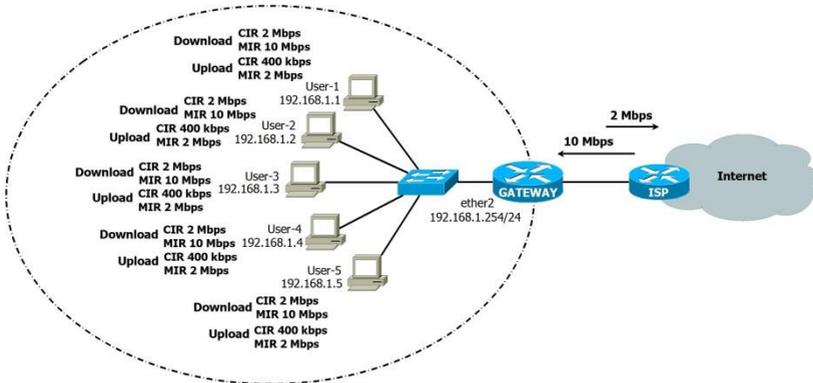
Dari gambar 7.2, terlihat konfigurasi Simple Queue memiliki 3 (tiga) konfigurasi queue. Queue pertama diberi nama *all-limit*, queue ini merupakan inner queue yang berfungsi untuk melakukan distribusi bandwidth kepada 2 (dua) queue yang berada di bawahnya. Queue *all-limit* ini memiliki 2 (dua) child, masing-masing adalah queue dengan nama *user-1* dan *user-2*. Adapun queue dengan nama *user-1* merupakan leaf queue yang bertugas memberikan alokasi bandwidth kepada komputer 192.168.1.1. Queue *user-1* ini merupakan leaf queue karena tidak lagi memiliki child (karena berada pada susunan paling bawah dari hirarki queue). Adapun queue *user-2* juga merupakan leaf queue dengan tugas memberikan alokasi bandwidth pada komputer 192.168.1.2.

Konfigurasi Dasar

Pada sub bab ini akan dibahas konfigurasi manajemen bandwidth dengan menggunakan Simple Queue. Konfigurasi yang akan digunakan adalah konfigurasi sederhana. Meskipun sederhana, pembahasan konfigurasi pada bab ini merupakan pembahasan mendasar yang sangat penting. Karena sangat mendasar dan nantinya akan menjadi acuan untuk konfigurasi yang lebih rumit, Anda dituntut untuk bisa memahami bagaimana memberikan nilai CIR dan MIR pada konfigurasi sederhana ini.

Topologi

Topologi yang digunakan adalah Router Gateway dengan jaringan 192.168.1.0/24. Pada jaringan tersebut terdapat 5 (lima) unit komputer user, masing-masing adalah *user-1*, *user-2* dan seterusnya. Adapun alokasi bandwidth yang didapatkan dari ISP adalah 10 Mbps untuk download dan 2 Mbps untuk upload. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 7.3
Jaringan 192.168.1.0/24 dengan alokasi bandwidth dari ISP

Sebelum melakukan konfigurasi Simple Queue, sebaiknya dilakukan perencanaan nilai CIR dan MIR yang akan didapatkan oleh masing-masing user. Untuk contoh skenario ini, alokasi bandwidth download dan upload akan dibagi secara merata. Untuk alokasi bandwidth download sebesar 10 Mbps, jika semua user akan menggunakan alokasi bandwidthnya, maka masing-masing user akan mendapatkan 2 Mbps (10 Mbps dibagi 5 komputer user). Sedangkan untuk alokasi upload, jika semua user melakukan aktifitas upload, maka masing-masing user akan mendapatkan 400 kbps (2 Mbps dibagi 5 komputer user).

Untuk mempermudah perhitungannya, pembagian alokasi CIR dan MIR untuk masing-masing user dapat dilihat pada tabel berikut ini.

Tabel 7.1
Pembagian bandwidth untuk jaringan 192.168.1.0/24

User	Download (10 Mbps dari ISP)		Upload (2 Mbps dari ISP)	
	CIR	MIR	CIR	MIR
user-1	2 Mbps	10 Mbps	400 kbps	2 Mbps
user-2	2 Mbps	10 Mbps	400 kbps	2 Mbps
user-3	2 Mbps	10 Mbps	400 kbps	2 Mbps
user-4	2 Mbps	10 Mbps	400 kbps	2 Mbps
user-5	2 Mbps	10 Mbps	400 kbps	2 Mbps

Dari tabel 7.1, terlihat bahwa setiap user akan mendapatkan alokasi CIR 2 Mbps dan MIR 10 Mbps untuk bandwidth download-nya. Sedangkan untuk alokasi upload-nya, setiap user akan mendapatkan CIR sebesar 400 kbps dan MIR 2 Mbps.

Sebagai panduan singkat, untuk mendapatkan nilai CIR, Anda dapat melakukan perhitungan dengan cara membagi alokasi bandwidth dari ISP dengan jumlah user yang ada. Sebagai contoh, untuk mendapatkan nilai CIR download, perhitungan yang dilakukan adalah membagi alokasi bandwidth 10 Mbps dari ISP dengan jumlah user. Karena pada jaringan tersebut terdapat 5 (lima) user, maka alokasi 10 Mbps tersebut dibagi 5, sehingga didapatkan nilai 2 Mbps. Nilai 2 Mbps inilah yang menjadi alokasi CIR untuk download. Perhitungan yang sama dapat digunakan untuk mencari nilai CIR upload.

Sebagai catatan, contoh pembagian pada tabel 7.1 merupakan pembagian yang merata. Anda bisa saja melakukan pembagian alokasi bandwidth yang tidak merata sehingga bisa saja Anda membuat setiap user akan mendapatkan nilai CIR dan MIR yang tidak sama.

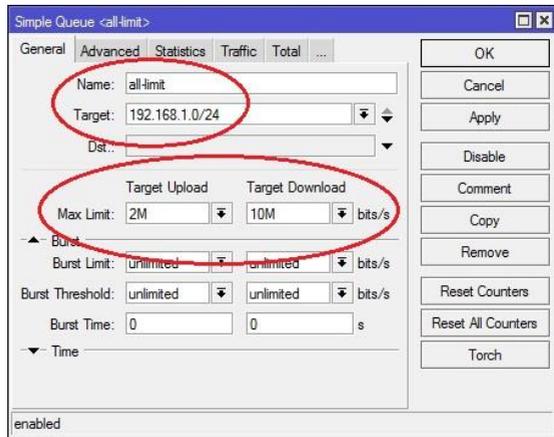
Konfigurasi Simple Queue

Langkah pertama untuk menerapkan manajemen bandwidth sesuai gambar 7.3 dan tabel 7.1 adalah membuat inner queue terlebih dahulu. Inner queue ini bertugas untuk melakukan distribusi atau pembagian bandwidth pada jaringan 192.168.1.0/24. Pada saat melakukan konfigurasi inner queue ini, harus digunakan parameter *max-limit=2M/10M*. Nilai parameter ini disesuaikan dengan alokasi bandwidth upload 2 Mbps dan download 10 Mbps yang didapatkan dari ISP. Adapun perintah yang digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=all-limit \
target=192.168.1.0/24 max-limit=2M/10M
```

```
[admin@GATEWAY] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
 0 name="all-limit" target=192.168.1.0/24 parent=none
  packet-marks="" priority=8/8 queue=default-small/default-
  small limit-at=0/0 max-limit=2M/10M burst-limit=0/0
  burst-threshold=0/0 burst-time=0s/0s bucket-size=0.1/0.1
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Queues** → tab **Simple Queues**, tombol **Add** → tab **General**, seperti pada gambar berikut ini.

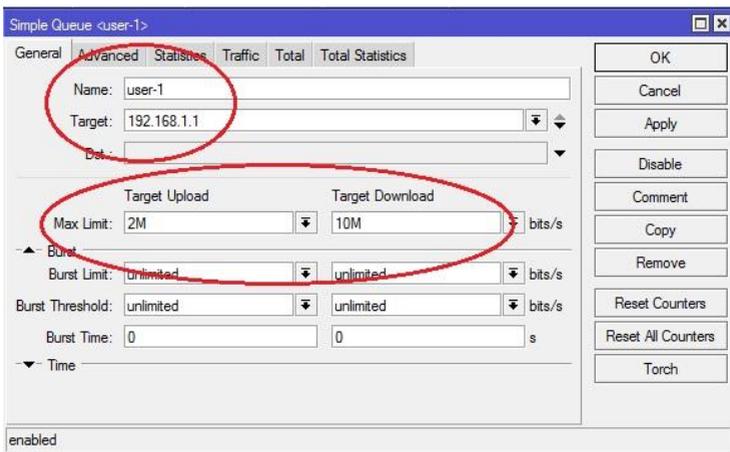


Gambar 7.4
Konfigurasi Inner
Queue untuk jaringan
192.168.1.0/24

Selanjutnya adalah membuat konfigurasi leaf queue untuk komputer *user-1* yang memiliki IP Address 192.168.1.1. Pada saat melakukan konfigurasi leaf queue ini, akan digunakan parameter *max-limit=2M/10M* yang akan menentukan nilai MIR upload dan download untuk user tersebut. Sedangkan parameter lain yang digunakan adalah *limit-at=400k/2M* yang akan menentukan nilai CIR upload/download yang akan didapatkan oleh user tersebut. Selain itu juga harus digunakan parameter *parent=all-limit* yang menentukan queue mana yang akan menjadi parent (inner queue). Adapun perintah leaf queue untuk komputer *user-1* adalah sebagai berikut.

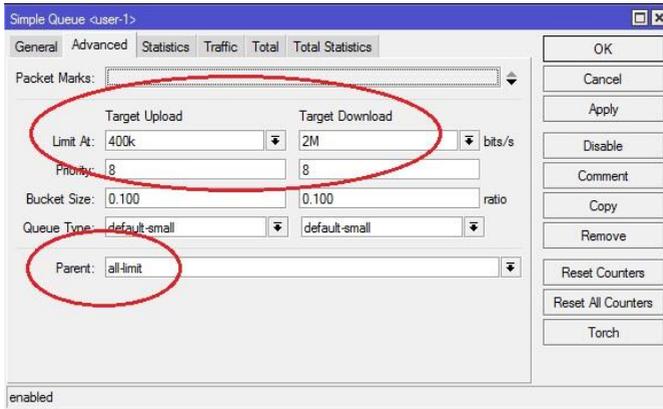
```
[admin@GATEWAY] > queue simple add name=user-1          \  
target=192.168.1.1 max-limit=2M/10M limit-at=400k/2M    \  
parent=all-limit
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Queues** → tab **Simple Queues**, tombol **Add** → tab **General**, seperti pada gambar berikut ini.



Gambar 7.5
Leaf queue untuk *user-1*

Adapun parameter *limit-at* dan *parent*, dapat dikonfigurasi pada tab **Advanced**, seperti pada gambar berikut ini.



Gambar 7.6
Parameter *limit-at* dan *parent* untuk queue user-1

Adapun konfigurasi leaf queue untuk *user-2*, *user-3*, *user-4* dan *user-5*, dapat menggunakan perintah berikut ini.

```
[admin@GATEWAY] > queue simple add name=user-2          \  
target=192.168.1.2 max-limit=2M/10M limit-at=400k/2M  \  
parent=all-limit  
  
[admin@GATEWAY] > queue simple add name=user-3          \  
target=192.168.1.3 max-limit=2M/10M limit-at=400k/2M  \  
parent=all-limit  
  
[admin@GATEWAY] > queue simple add name=user-4          \  
target=192.168.1.4 max-limit=2M/10M limit-at=400k/2M  \  
parent=all-limit  
  
[admin@GATEWAY] > queue simple add name=user-5          \  
target=192.168.1.5 max-limit=2M/10M limit-at=400k/2M  \  
parent=all-limit
```

Setelah semua konfigurasi dilakukan, maka seharusnya pada menu **Queues** → tab **Simple Queues**, akan terlihat konfigurasi queue seperti pada gambar berikut ini, perhatikanlah susunan hirarki pada konfigurasi tersebut, terdapat 1 (satu) inner queue dan 5 (lima) leaf queue.

#	me	Target	Upload Max Limit	Download Max Limit	Upload Limit At	Download Limit At
0	all-limit	192.168.1.0/24	2M	10M	unlimited	unlimited
1	user-1	192.168.1.1	2M	10M	400k	2M
2	user-2	192.168.1.2	2M	10M	400k	2M
3	user-3	192.168.1.3	2M	10M	400k	2M
4	user-4	192.168.1.4	2M	10M	400k	2M
5	user-5	192.168.1.5	2M	10M	400k	2M

Gambar 7.7
Susunan konfigurasi Simple Queue untuk jaringan 192.168.1.0/24

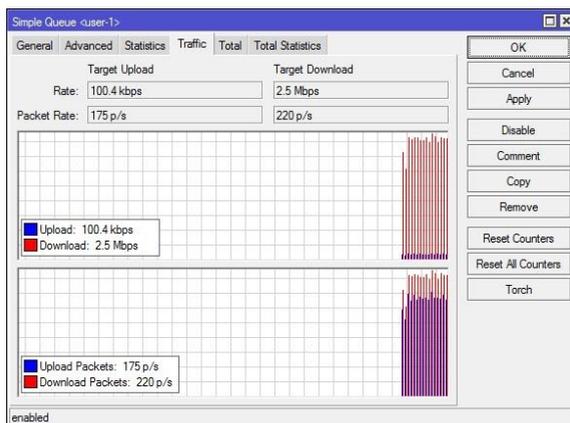
Pengujian Awal

Setelah konfigurasi semua selesai dilakukan, maka perlu dilakukan pengujian awal. Pengujian awal dapat dilakukan dengan melakukan aktifitas Internet pada masing-masing komputer user.

Sebagai contoh, Anda bisa melakukan aktifitas browsing pada *user-1* dan kemudian mengamati konfigurasi pada Simple Queue. Jika ternyata *user-1* sedang menggunakan Internet, maka nilai parameter *rate* pada konfigurasi leaf queue milik *user-1* harus memperlihatkan nilai tertentu. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple print detail rate
Flags: X - disabled, I - invalid, D - dynamic
#   NAME           TARGET           RATE                TOTAL-RATE
0   all-limit      192.168.1.0/24  101.4 kbps/2.3Mbps  0bps
1   user-1         192.168.1.1/32  101.4 kbps/2.3Mbps  0bps
2   user-2         192.168.1.2/32  0bps/0bps           0bps
3   user-3         192.168.1.3/32  0bps/0bps           0bps
4   user-4         192.168.1.4/32  0bps/0bps           0bps
5   user-5         192.168.1.5/32  0bps/0bps           0bps
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Queues** → tab **Simple Queue**, klik 2x leaf queue *user-1*, kemudian memilih tab **Traffic**, seperti pada gambar berikut ini.



Gambar 7.8
Aktifitas pemakaian bandwidth dari user-1

Jika pada pengujian awal ini, nilai *rate* tidak terlihat atau bernilai 0, maka bisa dipastikan bahwa konfigurasi Simple Queue yang dilakukan tidak tepat.

Pengujian ini harus dilakukan pada konfigurasi leaf queue untuk komputer *user-2*, *user-3* dan seterusnya. Harus dipastikan pula bahwa jika parameter *rate* pada konfigurasi leaf queue memiliki nilai, maka parameter *rate* pada inner queue juga memiliki nilai tertentu. Jika ternyata parameter *rate* pada leaf queue memiliki nilai tertentu sedangkan parameter *rate* pada inner queue bernilai 0, maka konfigurasi Simple Queue yang dilakukan juga terdapat kesalahan.

Setelah pengujian awal dilakukan dan sudah bisa dipastikan bahwa konfigurasi leaf queue sudah bekerja. Harus dilakukan pengujian lanjutan untuk memastikan apakah distribusi atau pembagian bandwidth bisa berjalan. Juga untuk memastikan nilai CIR dan MIR

yang akan didapatkan seorang user. Pengujian lanjutan ini akan dibahas pada sub bab selanjutnya.

Pengujian

Setelah dipastikan bahwa inner queue dan leaf queue untuk masing-masing user bisa bekerja, maka seharusnya dilakukan pengujian lanjutan yang lebih lengkap. Pengujian ini bertujuan untuk memastikan apakah setiap user bisa mendapatkan alokasi CIR maupun MIR sesuai perencanaan awal. Untuk melakukan pengujian ini, maka aktifitas download maupun upload dari setiap komputer user harus dimaksimalkan.

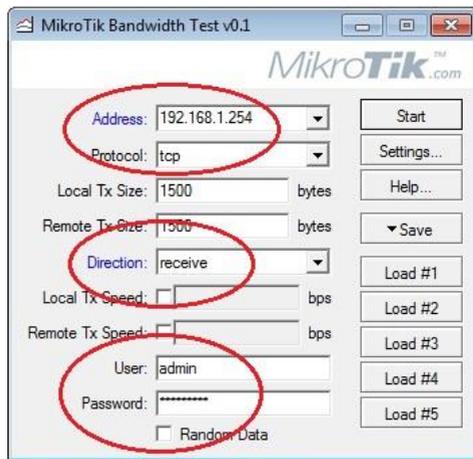
Untuk memaksimalkan aktifitas download maupun upload, salah satu cara yang dapat ditempuh adalah dengan melakukan download file-file dengan ukuran besar yang ada di Internet. Sedangkan untuk pengujian upload, setiap komputer user harus diusahakan untuk melakukan upload file-file dengan ukuran besar ke server-server yang ada di Internet. Namun, jika aktifitas download maupun upload file-file besar tersebut sedikit menyulitkan Anda, maka MikroTik sudah menyediakan aplikasi bandwidth test (btest.exe).

Bandwidth Test

Aplikasi Bandwidth Test dapat digunakan untuk menggantikan aktifitas download maupun upload yang dilakukan oleh komputer user. Aplikasi ini hanya dapat dijalankan pada komputer user yang menggunakan sistem operasi Windows. Saat dijalankan, aplikasi ini bisa menghasilkan traffic yang besar, baik itu traffic upload maupun traffic download. Aplikasi ini hanya bisa digunakan untuk menguji alokasi bandwidth yang diberikan oleh Router MikroTik, tidak untuk router jenis lain. Ini karena saat dijalankan, aplikasi

Bandwidth Test sebenarnya akan membuat koneksi upload maupun download ke Router MikroTik.

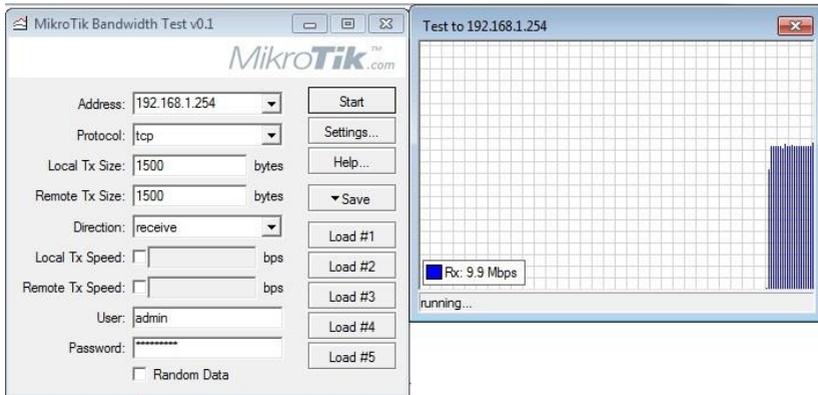
Aplikasi Bandwidth Test ini dapat di-download pada alamat <http://www.mikrotik.co.id/download.php>. Proses instalasi tidak diperlukan untuk menjalankan aplikasi ini, sesaat setelah di-download, Anda dapat menjalankannya, seperti pada gambar berikut ini.



Gambar 7.9
Aplikasi btest

Dari gambar 7.9, untuk menjalankan aplikasi ini, harus diketahui username dan password yang ada di Router MikroTik tempat titik acuan pengujian dilakukan. Jika mengacu pada gambar 7.3, maka username dan password dari Router Gateway harus diketahui. Adapun parameter *address*, dapat menggunakan IP Address 192.168.1.254 yang ada pada interface *ether2*. Selanjutnya, untuk menguji alokasi bandwidth download yang didapatkan oleh komputer user, maka pilihan parameter *direction* adalah *receive*, sedangkan untuk alokasi upload adalah *send*. Adapun parameter *protocol* yang sebaiknya digunakan adalah *tcp*.

Gambar berikut memperlihatkan bahwa *user-1* sedang mendapatkan alokasi bandwidth download 9,9 Mbps.



Gambar 7.10
User-1 mendapatkan alokasi download 9,9 Mbps

speedtest.net

Selain menggunakan *bttest.exe*, Anda juga bisa melakukan pengujian dari komputer user dengan menggunakan web site **speedtest.net**. Web site ini menyediakan pengujian alokasi bandwidth download maupun upload. Untuk menggunakan layanannya, Anda tinggal membuka browser dan mengetikkan alamat <https://www.speedtest.net>, seperti terlihat pada gambar berikut ini.



Gambar 7.11
Web Speedtest.net

Dari gambar 7.11, Anda tinggal meng-klik tombol Go untuk melakukan pengujian. Terlihat bahwa *user-1* mendapatkan alokasi download 9,78 Mbps dan upload 1,34 Mbps.

Sebagai catatan, karena titik acuan pengujian speedtest berada pada lokasi server yang berbeda-beda, maka bisa saja pengujian dengan speedtest ini akan memperlihatkan hasil yang berbeda-beda, jika dilakukan pada titik acuan server yang berbeda pula.

Torch

Setelah Anda mengetahui cara-cara membangkitkan traffic, baik itu dengan menggunakan aktifitas Internet biasa, menggunakan btest maupun menggunakan speedtest, maka tahapan selanjutnya adalah melakukan pengujian alokasi bandwidth CIR maupun MIR. Untuk pengujian ini, Router MikroTik memiliki fitur **Torch** yang bisa memperlihatkan alokasi upload maupun download (secara realtime) yang didapatkan komputer user.

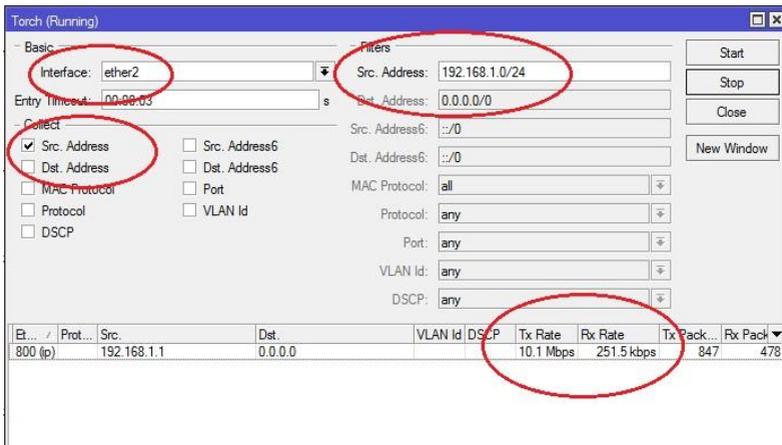
Sebagai contoh pengujian, skenario jaringan dan konfigurasi yang digunakan adalah skenario jaringan pada gambar 7.3, dimana terdapat 5 (lima) user dengan alokasi bandwidth download 10 Mbps dan upload 2 Mbps dari ISP.

Untuk mendapatkan alokasi MIR dari komputer *user-1*, dapat dilakukan aktifitas upload maupun download dari komputer tersebut. Sebagai contoh, jika hanya komputer *user-1* yang melakukan aktifitas download, maka alokasi yang didapatkan adalah 10 Mbps. Dengan menggunakan *torch*, alokasi ini dapat dilihat dengan menggunakan perintah berikut ini. Perhatikanlah penggunaan parameter *interface=ether2*, dimana komputer *user-1* terhubung.

```
[admin@GATEWAY] > tool torch interface=ether2
src-address=192.168.1.0/24
```

```
MAC-P SRC-ADDRESS TX RX TX-PACKETS RX-PACKETS
ip 192.168.1.1 10.1Mbps 235.2kbps 843 476
10.1Mbps 235.2kbps 843 476
-- [Q quit|D dump|C-z pause]
```

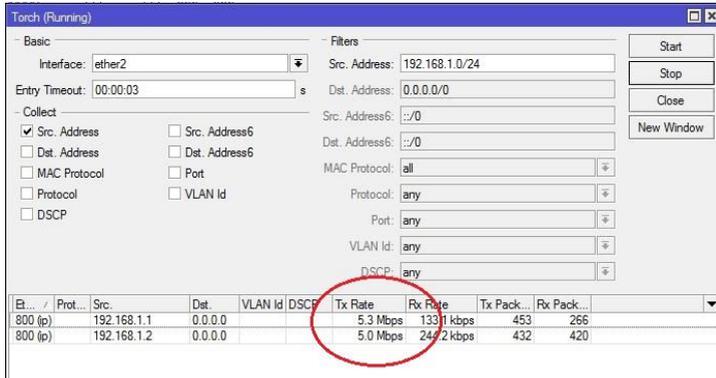
Dengan menggunakan WinBox, menu yang dapat digunakan adalah menu **Tools** → **Torch**, tombol **Start**, seperti pada gambar berikut ini.



Gambar 7.12

user-1 mendapatkan alokasi download 10,1 Mbps

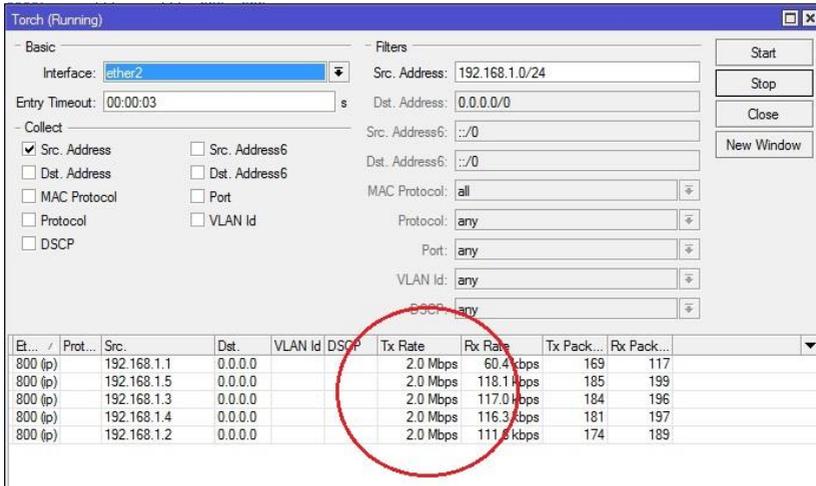
Pengujian selanjutnya dapat dijalankan dengan melakukan aktifitas download dari komputer *user-1* dan *user-2* secara bersamaan. Jika ternyata kedua komputer melakukan aktifitas download, maka seharusnya alokasi download yang didapatkan oleh masing-masing user adalah sekitar 5 Mbps, seperti terlihat pada gambar berikut ini.



Gambar 7.13

user-1 dan user-2 masing-masing mendapatkan alokasi sekitar 5 Mbps

Bagaimana jika keseluruhan 5 (lima) komputer user melakukan aktifitas download-nya? Pada kondisi ini, setiap komputer akan mendapatkan alokasi bandwidth terendahnya, atau akan mendapatkan nilai CIR-nya sebesar 2 Mbps, seperti terlihat pada gambar berikut ini.



Gambar 7.14

Semua user mendapatkan alokasi CIR

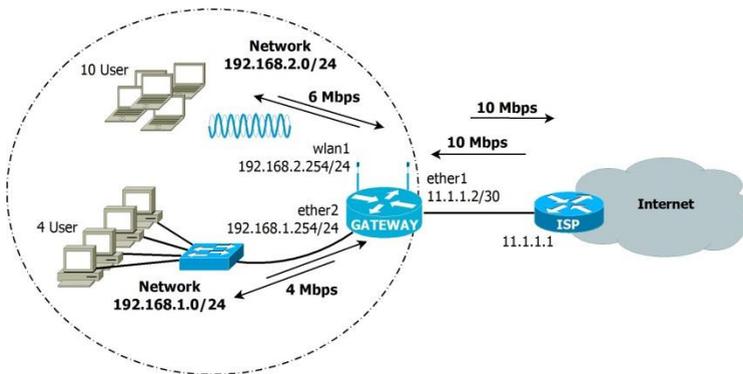
Dari uraian di atas, dapat disimpulkan bahwa pengujian bisa dilakukan dengan berbagai macam metode dan selama pengujian berlangsung, alokasi bandwidth dapat dimonitor dengan menggunakan fitur **Torch**. Tentunya Anda dapat melakukan berbagai macam skenario aktifitas download maupun upload sambil memperhatikan data penggunaan bandwidth yang ditampilkan oleh **Torch**.

Multiple Network

Pada sub bab ini akan dibahas sebuah contoh skenario jaringan yang sedikit berbeda. Pembahasan ini bertujuan untuk memperlihatkan contoh konfigurasi manajemen bandwidth dimana sebuah Router MikroTik memiliki beberapa jaringan lokal yang terhubung pada interface yang berbeda.

Topologi

Adapun topologi yang digunakan dapat dilihat pada gambar berikut ini.



Gambar 7.15
Router Gateway memiliki 2 (dua) jaringan lokal

Dari gambar 7.15, terlihat bahwa Router Gateway memiliki 2 (dua) jaringan lokal. Kedua jaringan tersebut, masing-masing adalah jaringan 192.168.1.0/24 pada interface *ether2* dan jaringan 192.168.2.0/24 pada interface *wlan1* (wireless). Pada jaringan 192.168.1.0/24 terdapat 4 (empat) unit komputer sedangkan pada 192.168.2.0/24 terdapat 10 (sepuluh) unit komputer. Adapun pembagian CIR dan MIR sudah dilakukan pada level jaringan, terlihat bahwa jaringan 192.168.1.0/24 mendapatkan nilai CIR 4

Mbps dan MIR 10 Mbps untuk alokasi download, sedangkan jaringan 192.168.2.0/24 mendapatkan 6 Mbps dan 10 Mbps. Alokasi CIR dan MIR untuk level jaringan dapat ditabelkan seperti berikut ini.

Tabel 7.2
Alokasi CIR dan MIR untuk 2 (dua) jaringan

Jaringan		Upload (10 Mbps)		Download (10 Mbps)	
		CIR	MIR	CIR	MIR
192.168.1.0/24		4 Mbps	10 Mbps	4 Mbps	10 Mbps
	Wired-1	1 Mbps	10 Mbps	1 Mbps	10 Mbps
	Wired-2	1 Mbps	10 Mbps	1 Mbps	10 Mbps
	Wired-3	1 Mbps	10 Mbps	1 Mbps	10 Mbps
	Wired-4	1 Mbps	10 Mbps	1 Mbps	10 Mbps
192.168.2.0/24		6 Mbps	10 Mbps	6 Mbps	10 Mbps
	Wireless-1	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-2	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-3	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-4	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-5	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-6	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-7	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-8	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-9	600kbps	10 Mbps	600kbps	10 Mbps
	Wireless-10	600kbps	10 Mbps	600kbps	10 Mbps

Dari tabel 7.2 terlihat bahwa masing-masing jaringan sudah mendapatkan alokasi CIR dan MIR-nya terlebih dahulu. Terlihat bahwa jaringan kabel mendapatkan CIR 4 Mbps dan MIR 10 Mbps, sedangkan jaringan wireless mendapatkan alokasi CIR 6 Mbps dan MIR 10 Mbps. Untuk skenario ini alokasi download maupun upload mendapatkan perhitungan yang sama, terlihat ISP memberikan alokasi 10 Mbps untuk upload dan 10 Mbps untuk download. Dari tabel tersebut juga terlihat, bahwa setelah perhitungan CIR dan MIR dilakukan untuk tingkatan jaringan, maka alokasi CIR dan MIR

untuk setiap user yang ada di masing-masing jaringan juga harus diperhitungkan.

Sebagai catatan penting, jumlah total nilai CIR dari keseluruhan user yang ada pada suatu jaringan tidak boleh melebihi dari nilai CIR yang diberikan pada jaringan tersebut. Sebagai contoh, jika CIR dari alokasi download *wired-1*, *wired-2*, *wired-3* dan *wired-4* dijumlahkan, tidak boleh melebihi nilai CIR yang diberikan kepada network 192.168.1.0/24. Begitu juga untuk semua user wireless yang ada pada jaringan 192.168.2.0/24, jumlah keseluruhan CIR user wireless tidak bisa melebihi nilai CIR yang sudah diberikan kepada jaringan 192.168.2.0/24.

Konfigurasi

Tahapan konfigurasi skenario pada sub bab ini akan mengikuti alokasi yang sudah diberikan pada tabel 7.2. Langkah pertama adalah membuat konfigurasi inner queue yang bertugas untuk melakukan distribusi bandwidth kepada jaringan kabel (*wired*) dan jaringan wireless, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=all-limit          \  
target=0.0.0.0/0 max-limit=10M/10M
```

Selanjutnya adalah membuat konfigurasi inner queue untuk distribusi bandwidth bagi jaringan wired 192.168.1.0/24, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=wired-limit        \  
target=192.168.1.0/24 max-limit=10M/10M limit-at=4M/4M    \  
parent=all-limit
```

Sedangkan konfigurasi inner queue untuk distribusi bandwidth ke jaringan wireless 192.168.2.0/24, dapat menggunakan perintah berikut ini.

```
[admin@GATEWAY] > queue simple add name=wireless-limit \
target=192.168.2.0/24 max-limit=10M/10M limit-at=6M/6M \
parent=all-limit
```

Langkah berikutnya adalah membuat konfigurasi leaf queue bagi masing-masing user yang pada jaringan wired 192.168.1.0/24. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=wired-1 \
target=192.168.1.1 max-limit=10M/10M limit-at=1M/1M \
parent=wired-limit
```

```
[admin@GATEWAY] > queue simple add name=wired-2 \
target=192.168.1.2 max-limit=10M/10M limit-at=1M/1M \
parent=wired-limit
```

```
[admin@GATEWAY] > queue simple add name=wired-3 \
target=192.168.1.3 max-limit=10M/10M limit-at=1M/1M \
parent=wired-limit
```

```
[admin@GATEWAY] > queue simple add name=wired-4 \
target=192.168.1.4 max-limit=10M/10M limit-at=1M/1M \
parent=wired-limit
```

Yang terakhir adalah konfigurasi leaf queue bagi user yang ada pada jaringan wireless 192.168.2.0/24. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=wireless-1 \
target=192.168.2.1 max-limit=10M/10M limit-at=600k/600k \
parent=wireless-limit
```

```
[admin@GATEWAY] > queue simple add name=wireless-2 \
target=192.168.2.2 max-limit=10M/10M limit-at=600k/600k \
parent=wireless-limit
```

```
[admin@GATEWAY] > queue simple add name=wireless-3 \
target=192.168.2.3 max-limit=10M/10M limit-at=600k/600k \
parent=wireless-limit
```

```
[admin@GATEWAY] > queue simple add name=wireless-4          \  
target=192.168.2.4 max-limit=10M/10M limit-at=600k/600k   \  
parent=wireless-limit  
  
[admin@GATEWAY] > queue simple add name=wireless-5          \  
target=192.168.2.5 max-limit=10M/10M limit-at=600k/600k   \  
parent=wireless-limit  
  
[admin@GATEWAY] > queue simple add name=wireless-6          \  
target=192.168.2.6 max-limit=10M/10M limit-at=600k/600k   \  
parent=wireless-limit  
  
[admin@GATEWAY] > queue simple add name=wireless-7          \  
target=192.168.2.7 max-limit=10M/10M limit-at=600k/600k   \  
parent=wireless-limit  
[admin@GATEWAY] > queue simple add name=wireless-8          \  
target=192.168.2.8 max-limit=10M/10M limit-at=600k/600k   \  
parent=wireless-limit  
  
[admin@GATEWAY] > queue simple add name=wireless-9          \  
target=192.168.2.9 max-limit=10M/10M limit-at=600k/600k   \  
parent=wireless-limit  
  
[admin@GATEWAY] > queue simple add name=wireless-10        \  
target=192.168.2.10 max-limit=10M/10M limit-at=600k/600k  \  
parent=wireless-limit
```

Setelah semua konfigurasi selesai, maka susunan queue pada Simple Queue seharusnya terlihat seperti gambar berikut ini.

#	Name	Target	Download Max Limit	Download Limit At	Total Max L
0	all-limit	0.0.0.0/0	10M	unlimited	
1	wired-limit	192.168.1.0/24	10M	4M	
3	wired-1	192.168.1.1	10M	1M	
4	wired-2	192.168.1.2	10M	1M	
5	wired-3	192.168.1.3	10M	1M	
6	wired-4	192.168.1.4	10M	1M	
2	wireless-limit	192.168.2.0/24	10M	6M	
7	wireless-1	192.168.2.1	10M	600k	
8	wireless-2	192.168.2.2	10M	600k	
9	wireless-3	192.168.2.3	10M	600k	
10	wireless-4	192.168.2.4	10M	600k	
11	wireless-5	192.168.2.5	10M	600k	
12	wireless-6	192.168.2.6	10M	600k	
13	wireless-7	192.168.2.7	10M	600k	
14	wireless-8	192.168.2.8	10M	600k	
15	wireless-9	192.168.2.9	10M	600k	
16	wireless-10	192.168.2.10	10M	600k	

Gambar 7.16
Susunan konfigurasi Queue untuk multiple LAN

Per Connection Queue (PCQ)

Dalam beberapa skenario, Anda akan menemukan jaringan dengan jumlah user yang relatif banyak, atau dengan jumlah user yang tidak pasti. Pada kondisi ini, menghitung nilai CIR untuk masing-masing user akan sangat merepotkan. Apalagi jika ternyata terdapat ratusan user, sehingga harus dibuat leaf queue dengan jumlah ratusan pula.

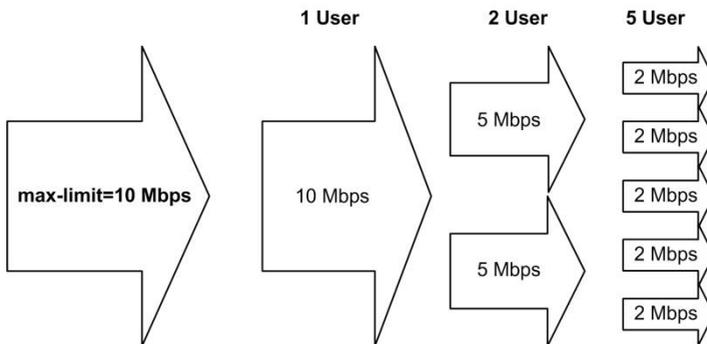
Untuk skenario seperti penjelasan tadi, Simple Queue membutuhkan tambahan parameter. Adapun tambahan konfigurasi ini bertujuan untuk melakukan sedikit perubahan metode queue yang akan digunakan. Dan metode queue yang dapat membantu adalah Per Connection Queue (PCQ). Metode queue ini merupakan metode

queue yang ditujukan untuk menangani user dalam jumlah yang banyak maupun jumlah yang tidak tetap.

Konsep Dasar PCQ

Per Connection Queue merupakan metode queue yang dimiliki oleh Router MikroTik yang dapat membagi alokasi bandwidth secara merata. Secara default, PCQ akan menghitung berapa berapa user yang ingin menggunakan alokasi bandwidth untuk kemudian membagi rata bandwidth yang tersedia, sesuai jumlah user yang ingin menggunakannya.

Sebagai contoh, jika suatu jaringan memiliki alokasi bandwidth 10 Mbps, dan ternyata hanya 1 user yang ingin menggunakan alokasi bandwidth, maka user tersebut akan mendapatkan 10 Mbps. Jika terdapat 2 user, maka masing-masing user akan mendapatkan 5 Mbps. Jika terdapat 10 user yang ingin menggunakan bandwidth, masing-masing user akan mendapatkan 1 Mbps, demikian seterusnya. Ilustrasinya dapat dilihat pada gambar berikut ini.



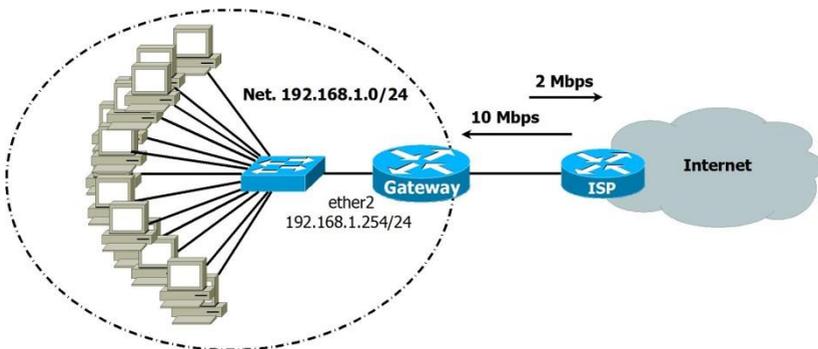
Gambar 7.17
PCQ membagi alokasi bandwidth secara merata

Yang perlu diingat saat menggunakan PCQ adalah resource memori dari Router MikroTik. Saat PCQ digunakan, Router MikroTik akan membutuhkan alokasi memori lebih banyak, dibandingkan jika Anda tidak menggunakan PCQ.

PCQ merupakan metode queue yang sangat lengkap untuk menangani skenario jaringan yang cenderung rumit. Terdapat banyak parameter yang dimiliki oleh PCQ. Namun, untuk kebutuhan konfigurasi di buku ini, yang digunakan adalah PCQ dengan parameter-parameter default saja. Penggunaan PCQ secara mendalam belum dibahas pada buku ini.

Skenario 1

Pada skenario pertama ini akan digunakan topologi dan skenario seperti yang ada pada gambar 7.3. Namun, untuk skenario kali ini, jumlah komputer yang ada pada jaringan tersebut tidak diketahui dengan pasti. Jika digambarkan kembali, maka topologinya akan terlihat seperti gambar berikut ini.



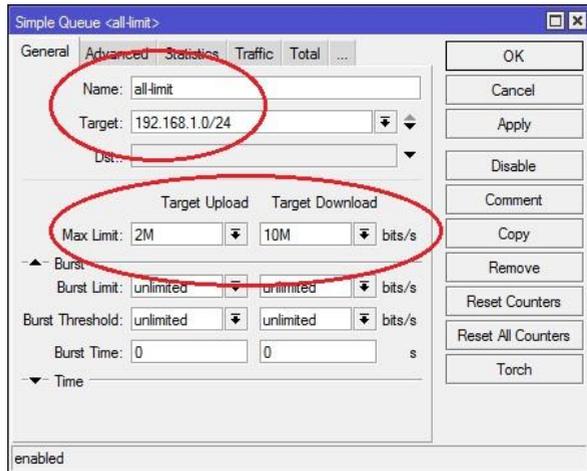
Gambar 7.18
Jaringan 192.168.1.0/24

Dari gambar di atas, alokasi bandwidth yang didapatkan dari ISP adalah 2 Mbps untuk upload dan 10 Mbps untuk download. Karena akan menggunakan PCQ, maka perhitungan nilai CIR maupun MIR secara detail tidak perlu dilakukan. Pembagian alokasi bandwidth akan dilakukan secara otomatis oleh PCQ. Adapun perintah yang dapat digunakan untuk melakukan manajemen bandwidth dengan menggunakan PCQ adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=all-limit \
target=192.168.1.0/24 max-limit=2M/10M \
queue=pcq-upload-default/pcq-download-default

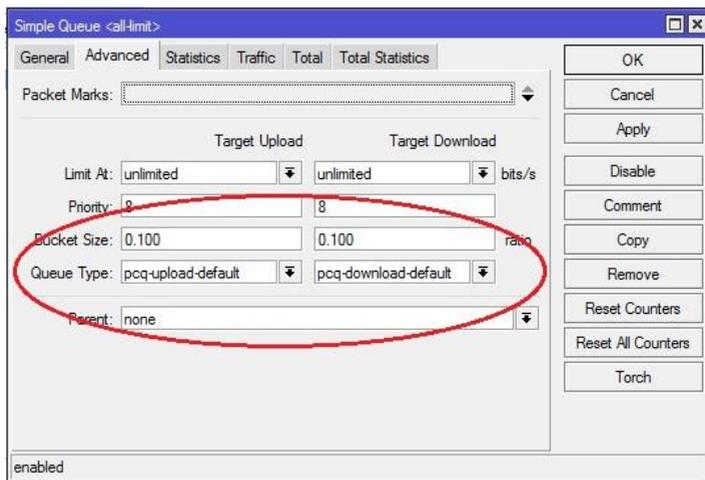
[admin@GATEWAY] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
 0 name="all-limit" target=192.168.1.0/24 parent=none
  packet-marks="" priority=8/8 queue=pcq-upload-
  default/pcq-download-default limit-at=0/0 max-
  limit=2M/10M burst-limit=0/0 burst-threshold=0/0 burst-
  time=0s/0s bucket-size=0.1/0.1
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Queues** → tab **Simple Queues** → tombol **Add**, seperti pada gambar berikut ini.



Gambar 7.19
Queue untuk
jaringan
192.168.1.0/24

Sedangkan parameter *queue* yang akan menggunakan PCQ, dapat dikonfigurasi pada tab **Advanced**, seperti pada gambar berikut ini.

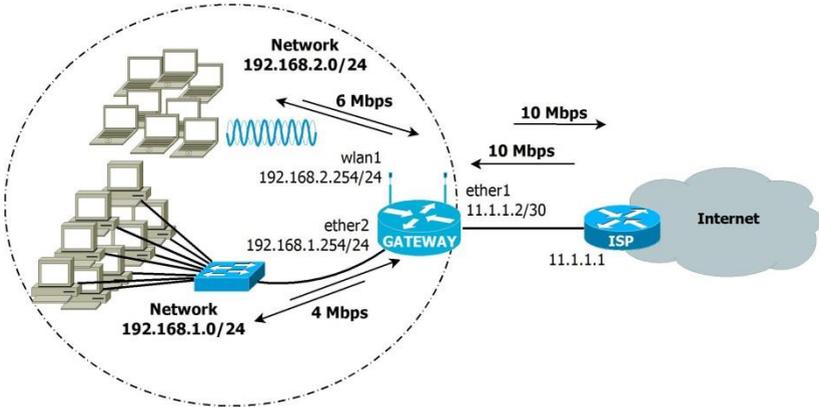


Gambar 7.20
Parameter *queue* menggunakan PCQ

Sampai pada tahapan ini, konfigurasi Simple Queue dengan menggunakan metode PCQ untuk jaringan 192.168.1.0/24 sudah selesai dilakukan ☺. Berapa pun jumlah komputer user yang ada pada jaringan tersebut, Anda tidak perlu repot-repot membuat konfigurasi queue yang banyak.

Skenario 2

Untuk contoh skenario kedua, akan digunakan topologi dengan multiple LAN, seperti terlihat pada gambar berikut ini.



Gambar 7.21

Jaringan wired 192.168.1.0/24 dan wireless 192.168.2.0/24

Pada gambar 7.21, perhitungan CIR dan MIR hanya dilakukan sampai pada tingkatan jaringan. Untuk pembagian bandwidth ditingkat user, akan dilakukan oleh PCQ. Dengan demikian, sebelum melakukan konfigurasi, hanya perlu dihitung nilai CIR dan MIR untuk jaringan 192.168.1.0/24 dan 192.168.2.0/24, seperti terlihat pada tabel berikut ini.

Tabel 7.3

Perhitungan CIR untuk jaringan 192.168.1.0/24 dan 192.168.2.0/24

Jaringan	Upload (10 Mbps)		Download (10 Mbps)	
	CIR	MIR	CIR	MIR
192.168.1.0/24	4 Mbps	10 Mbps	4 Mbps	10 Mbps
192.168.2.0/24	6 Mbps	10 Mbps	6 Mbps	10 Mbps

Langkah pertama adalah membuat konfigurasi inner queue untuk melakukan distribusi bandwidth kepada jaringan wired

192.168.1.0/24 dan wireless 192.168.2.0/24. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=all-limit \
target=0.0.0.0/0 max-limit=10M/10M
```

Selanjutnya adalah langsung membuat konfigurasi leaf queue untuk jaringan wired 192.168.1.0/24 dengan menggunakan PCQ sebagai metode queue-nya. Karena merupakan leaf queue maka konfigurasi ini akan langsung bertugas memberikan bandwidth kepada masing-masing user. Perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=wired-limit \
target=192.168.1.0/24 max-limit=10M/10M limit-at=4M/4M \
queue=pcq-upload-default/pcq-download-default \
parent=all-limit
```

Langkah terakhir adalah membuat konfigurasi leaf queue untuk jaringan wireless 192.168.2.0/24. Konfigurasi ini juga akan menggunakan PCQ, adapun perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > queue simple add name=wireless-limit \
target=192.168.2.0/24 max-limit=10M/10M limit-at=6M/6M \
queue=pcq-upload-default/pcq-download-default \
parent=all-limit
```

Setelah semua konfigurasi dilakukan, maka pada Simple Queue seharusnya terlihat konfigurasi seperti pada gambar berikut ini.

#	Name	Target	Download Max Limit	Download Limit At	Download Queue Type	Total M
0	all-limit	0.0.0.0/0	10M	unlimited	default-small	
1	wired-limit	192.168.1.0/24	10M	4M	pcq-download-default	
2	wireless-limit	192.168.2.0/24	10M	6M	pcq-download-default	

Gambar 7.22
Konfigurasi Queue dengan menggunakan PCQ

Dari gambar 7.22, terlihat bahwa dengan menggunakan PCQ, konfigurasi Simple Queue akan lebih mudah dilakukan. Konfigurasi untuk skenario ini cukup hanya membuat leaf queue sampai pada tingkat jaringan. Untuk kemudian pembagian bandwidth untuk masing-masing user akan dilakukan oleh PCQ. Anda dapat membandingkan gambar 7.22 ini dengan gambar 7.16. Perbandingan kedua gambar tersebut akan memperlihatkan konfigurasi yang tidak menggunakan PCQ dengan konfigurasi yang menggunakan PCQ.

End of Chapter

Bab 08

Switch Chip

Salah satu kelebihan dari Router MikroTik adalah router ini memiliki Switch Chip. Router MikroTik yang memiliki Switch Chip adalah beberapa seri RouterBoard. Switch Chip ini merupakan hardware yang sanggup menghadirkan fungsi switch di dalam sebuah router. Sehingga dalam beberapa skenario jaringan, Anda bisa menghemat anggaran untuk membeli sebuah switch. Memang tidak semua Router MikroTik memiliki fitur ini, namun untuk kebanyakan RouterBoard, hampir semuanya memiliki Switch Chip. Anda tinggal melihat data spesifikasi, apakah RouterBoard yang digunakan memiliki Switch Chip.

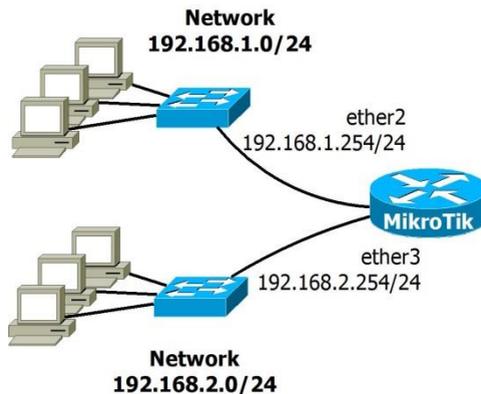
Fitur Switch Chip ini dapat dimanfaatkan untuk membangun jaringan dengan konsep Virtual Local Area Network (VLAN). Namun, pembahasan pada buku ini hanya meliputi bagaimana menggantikan fungsi Switch jika Router yang digunakan memiliki Switch Chip. Penerapan VLAN pada Switch Chip belum dibahas pada buku ini.

Prinsip Dasar Switch Chip

Sebelum melakukan konfigurasi untuk memanfaatkan Switch Chip pada RouterBoard, sangat dibutuhkan pemahaman perbedaan antara router dan switch. Tentunya juga harus dipahami proses yang dilakukan oleh router dan switch tadi. Garis besarnya adalah router akan melakukan proses routing sedangkan switch yang melakukan proses switching.

Router vs Switch

Secara mendasar, router adalah perangkat yang digunakan untuk menghubungkan komputer-komputer yang memiliki IP Address yang berbeda-beda. Dengan kata lain, router bertugas untuk menghubungkan komputer-komputer yang berasal dari jaringan yang berbeda-beda. Ilustrasinya dapat dilihat pada gambar berikut ini.

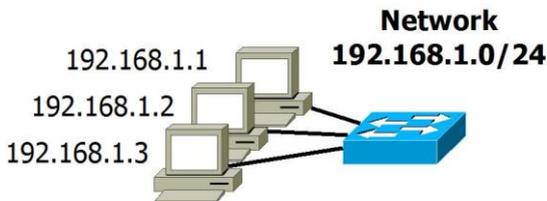


Gambar 8.1
Router menghubungkan 2 (dua) jaringan

Dari gambar 8.1, terlihat bahwa Router MikroTik menghubungkan komputer-komputer yang berasal dari 2 (dua) jaringan yang berbeda, masing-masing terlihat adalah jaringan 192.168.1.0/24 dan 192.168.2.0/24. Juga terlihat bahwa setiap interface dari router tersebut harus diberi IP Address, masing-masing adalah 192.168.1.254/24 pada interface *ether2* dan 192.168.2.254/24 pada interface *ether3*.

Sebagai catatan penting, untuk menghubungkan kedua jaringan tersebut, Router akan menggunakan Central Processing Unit (CPU) yang dimilikinya. Dengan kata lain, proses routing yang dilakukan oleh router akan menguras penggunaan CPU.

Bagaimana dengan Switch? Pada dasarnya, perangkat ini digunakan untuk menghubungkan komputer-komputer yang berasal dari jaringan yang sama. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 8.2
Switch pada jaringan 192.168.1.0/24

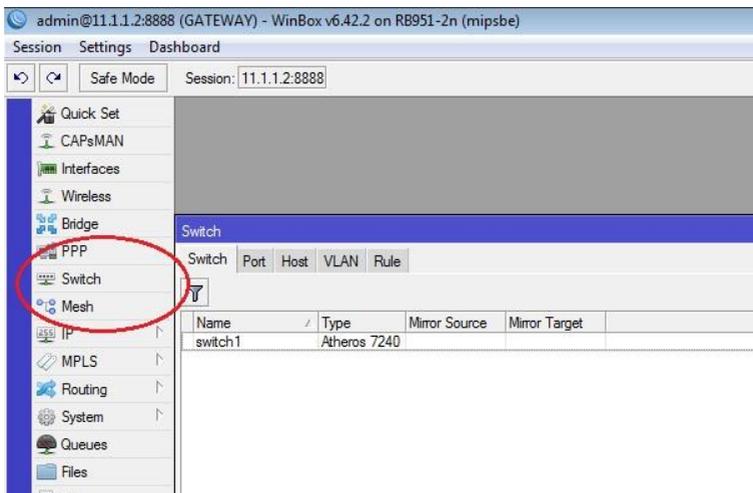
Dari gambar 8.2, terlihat sebuah switch menghubungkan beberapa komputer yang berasal dari jaringan yang sama, yaitu jaringan 192.168.1.0/24. Terlihat pula bahwa setiap port dari switch tidak membutuhkan IP Address sama sekali. Dan sebagai catatan penting lagi, proses switching tidak membutuhkan kinerja CPU, seperti pada proses routing. Dengan kata lain, proses switching dilakukan oleh hardware tersendiri sehingga tidak membutuhkan kinerja CPU.

Switch Chip pada RouterBoard

RouterBoard yang memiliki Switch Chip akan mampu melakukan proses switching, tentunya selain proses routing. Jika fitur Switch Chip ini digunakan maka beberapa interface dari RouterBoard akan dapat dialihkan fungsinya menjadi port switch.

Saat interface RouterBoard sudah menjadi port switch, maka interface tersebut tidak perlu lagi diberikan IP Address. Catatan lain yang penting adalah, fungsi-fungsi routing dan firewall pada port-port tersebut akan hilang.

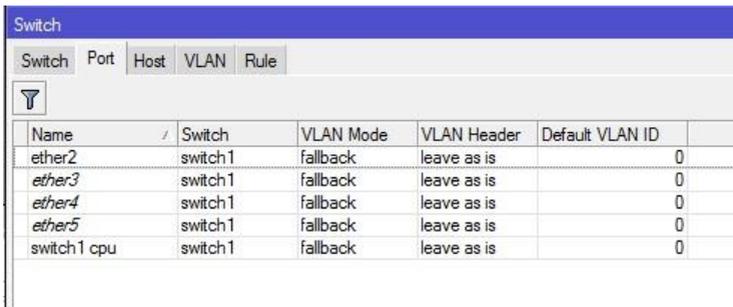
Karena tidak semua RouterBoard memiliki Switch Chip, maka penting untuk melihat ada tidaknya Switch Chip pada Router yang kita gunakan. RouterBoard yang memiliki Switch Chip akan memiliki menu Switch pada menu-menu yang ditampilkan oleh WinBox, seperti yang terlihat pada gambar berikut ini.



Gambar 8.3
Menu Switch pada WinBox

Untuk RouterBoard yang tidak memiliki Switch Chip, maka menu Switch tidak akan terlihat pada WinBox.

Selain itu harus diperhatikan pula, posisi atau keanggotaan setiap interface router terhadap Switch Chip. Interface yang tidak berada dalam satu Switch Chip, tidak akan bisa digabungkan untuk menjadi sebuah switch. Untuk melihat posisi interface terhadap Switch Chip, dapat digunakan menu **Switch** → tab **Ports**, seperti pada gambar berikut ini.



Name	Switch	VLAN Mode	VLAN Header	Default VLAN ID
ether2	switch1	fallback	leave as is	0
ether3	switch1	fallback	leave as is	0
ether4	switch1	fallback	leave as is	0
ether5	switch1	fallback	leave as is	0
switch1 cpu	switch1	fallback	leave as is	0

Gambar 8.4
Interface dan Switch Chip

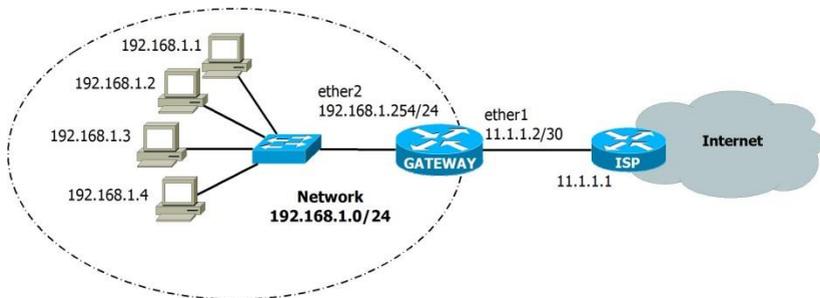
Dari gambar 8.4, terlihat bahwa Router MikroTik yang digunakan memilih sebuah Switch Chip yang diberi nama *switch1*. Dan interface-interface yang masuk ke dalam keanggotaan *switch1* adalah interface *ether2*, *ether3*, *ether4* dan *ether5*. Ini berarti keempat interface tersebut akan dapat digabungkan sehingga menjadi sebuah switch. Adapun interface *ether1* tidak masuk ke dalam *switch1*, ini membuat interface *ether1* tidak akan bisa digabungkan dengan interface lainnya untuk menjadi port switch.

Penerapan Switch Chip

Pada sub bab ini, akan dibahas 2 (dua) skenario jaringan yang akan memanfaatkan Switch Chip. Skenario yang akan digunakan adalah skenario sederhana dimana tujuan utama penggunaan Switch Chip adalah untuk menghilangkan kebutuhan perangkat Switch.

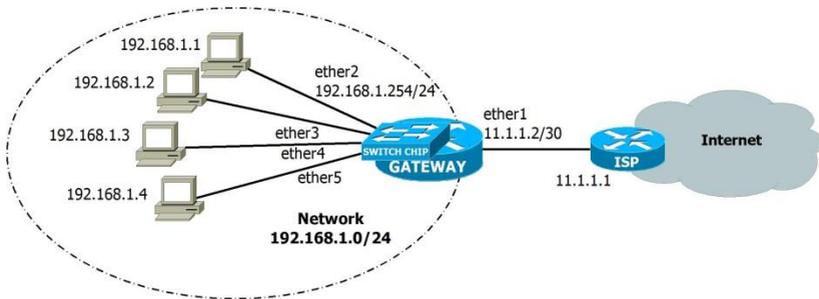
Skenario 1

Pada skenario pertama ini, terdapat sebuah jaringan dengan 4 (empat) unit komputer yang akan dihubungkan dengan Internet. Seperti jaringan pada umumnya, maka biasanya digunakan sebuah Switch untuk menghubungkan keempat komputer tersebut ke router. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 8.5
Switch pada jaringan 192.168.1.0/24

Untuk menghemat penggunaan Switch, maka fitur Switch Chip pada Router Gateway dapat diaktifkan. Switch Chip tersebut dapat membuat interface *ether2*, *ether3*, *ether4* dan *ether5* menjadi sebuah switch. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 8.6

Switch Chip pada Router Gateway untuk jaringan 192.168.1.0/24

Dari gambar 8.6, terlihat bahwa kebutuhan akan perangkat switch dapat dihindari dengan mengaktifkan Switch Chip pada Router Gateway. Terlihat pula bahwa interface *ether3*, *ether4* dan *ether5* tidak perlu diberikan IP Address. Yang perlu diberikan IP Address hanyalah interface *ether2*, selain tentunya interface *ether1* yang juga butuh IP Address untuk bisa terhubung ke ISP.

Untuk mewujudkan skenario pada gambar 8.6, perintah berikut ini dapat digunakan.

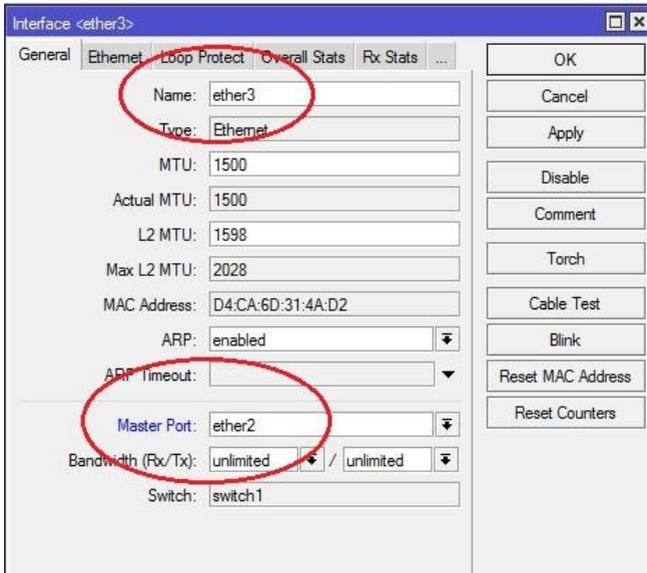
```
[admin@GATEWAY] > interface ethernet set ether3          \
master-port=ether2

[admin@GATEWAY] > interface ethernet set ether4          \
master-port=ether2

[admin@GATEWAY] > interface ethernet set ether5          \
master-port=ether2

[admin@GATEWAY] > interface ethernet print
Flags: X - disabled, R - running, S - slave
#  NAME      MTU  MAC-ADDRESS  ARP      MASTER-PORT  SWITCH
0  R  ether1    1500 D4:CA:6D:31: enabled  none          ether1
1  R  ether2    1500 D4:CA:6D:31: enabled  none          ether2
2  RS ether3    1500 D4:CA:6D:31: enabled  ether2       ether3
3  RS ether4    1500 D4:CA:6D:31: enabled  ether2       ether4
4  RS ether5    1500 D4:CA:6D:31: enabled  ether2       ether5
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Interfaces** → klik 2x interface *ether3*, pada tab **General**, parameter *master-port* dikonfigurasi pada interface *ether2*, seperti pada gambar berikut ini.



Gambar 8.7
Parameter *master-port* pada interface *ether3*

Selanjutnya, Anda tinggal mengulangi lagi konfigurasi pada WinBox, untuk interface *ether4* dan *ether5*. Kedua interface ini juga harus menggunakan interface *ether2* sebagai master port-nya.

Dari uraian konfigurasi di atas, terlihat bahwa interface *ether3*, *ether4* dan *ether5* akan menginduk ke interface *ether2*. Ketiga interface tersebut akan menggunakan interface *ether2* sebagai master port-nya. Terlihat pula bahwa interface *ether3*, *ether4* dan *ether5* akan memiliki label **S (Slave)**, seperti pada gambar berikut ini.

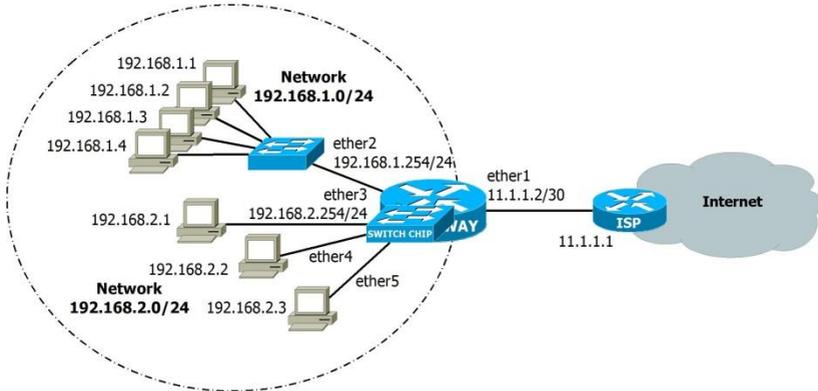
Interface List									
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRPP	Bonding	LTE
R	ether1	Ethernet	1500	1600			2.8 kbps		0 bps
R	ether2	Ethernet	1500	1598			73.7 kbps		10.0 kbps
RS	ether3	Ethernet	1500	1598			0 bps		0 bps
RS	ether4	Ethernet	1500	1598			0 bps		0 bps
RS	ether5	Ethernet	1500	1598			0 bps		0 bps
R	wlan1	Wireless (Atheros AR9...	1500	1600			2.8 kbps		0 bps

Gambar 8.8
Interface *ether3*, *ether4* dan *ether5* menjadi slave

Karena menjadi master port, maka interface *ether2* perlu diberikan IP Address dan DHCP Server. Konfigurasinya akan sama dengan konfigurasi yang sudah dibahas pada bab-bab sebelumnya. Begitu pula dengan konfigurasi default route, DNS, masquerade yang sama dengan konfigurasi-konfigurasi sebelumnya.

Skenario 2

Skenario kedua ini relatif sama dengan konfigurasi sebelumnya, hanya saja terdapat 2 (dua) jaringan yang akan dihubungkan ke Internet. Ilustrasinya dapat dilihat pada gambar berikut ini.



Gambar 8.9

Jaringan 192.168.2.0/24 menggunakan Switch Chip

Jaringan 192.168.2.0/24 hanya terdiri dari 3 (tiga) unit komputer. Dengan adanya Switch Chip pada Router Gateway maka kebutuhan switch pada jaringan tersebut dapat dihilangkan. Dengan Switch Chip, interface *ether3* bisa dijadikan master port, sedangkan interface *ether4* dan *ether5* akan menginduk kepada interface *ether3*. Adapun interface *ether2* tetap akan berdiri sendiri sebagai interface router

Untuk mewujudkan skenario pada gambar 8.9, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > interface ethernet set ether4          \
master-port=ether3

[admin@GATEWAY] > interface ethernet set ether5          \
master-port=ether3

[admin@GATEWAY] > interface ethernet print
Flags: X - disabled, R - running, S - slave
#  NAME      MTU  MAC-ADDRESS  ARP  MASTER-PORT  SWITCH
0  R  ether1    1500 D4:CA:6D:31: enabled  none
1  R  ether2    1500 D4:CA:6D:31: enabled  none          switch1
2  R  ether3    1500 D4:CA:6D:31: enabled  none          switch1
3  RS ether4    1500 D4:CA:6D:31: enabled  ether3        switch1
4  RS ether5    1500 D4:CA:6D:31: enabled  ether3        switch1
```

Setelah konfigurasi Switch Chip selesai dilakukan, maka label S akan terlihat pada interface *ether 4* dan *ether5*, seperti pada gambar berikut ini.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Pk
R	ether1	Ethernet	1500	1600	14.2 kbps	182.7 kbps	
R	ether2	Ethernet	1500	1598	386.7 kbps	33.5 kbps	
R	ether3	Ethernet	1500	1598	0 bps	0 bps	
RS	ether4	Ethernet	1500	1598	0 bps	0 bps	
RS	ether5	Ethernet	1500	1598	0 bps	0 bps	
R	wlan1	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	

Gambar 8.10
Interface *ether4* dan *ether5* memiliki label S

Konfigurasi Switch Chip di atas tentunya harus dilengkapi dengan konfigurasi IP Address pada interface *ether1*, *ether2* dan *ether3*. Begitu juga dengan kebutuhan DHCP Server pada interface *ether2* dan *ether3*, beserta konfigurasi-konfigurasi pelengkap lainnya.

End of Chapter

Bab 09

Manajemen Router

Selain melakukan konfigurasi yang berhubungan dengan layanan Internet, yang tidak kalah pentingnya adalah konfigurasi manajemen router itu sendiri. Manajemen router sebenarnya ditujukan untuk menghadirkan router yang berada dalam kondisi terbaik, sehingga akan memudahkan konfigurasi-konfigurasi lainnya. Manajemen router yang baik akan dihasilkan router yang sehat dan router yang sehat akan menghasilkan jaringan yang sehat dan kuat pula.

Backup dan Restore

Yang teramat penting saat mengoperasikan router adalah melakukan proses backup dan restore. Proses backup ini ditujukan untuk menyimpan semua konfigurasi yang sudah dilakukan, sehingga bila konfigurasi-konfigurasi tersebut dibutuhkan kembali, maka Anda tinggal melakukan proses pengembalian konfigurasi (restore).

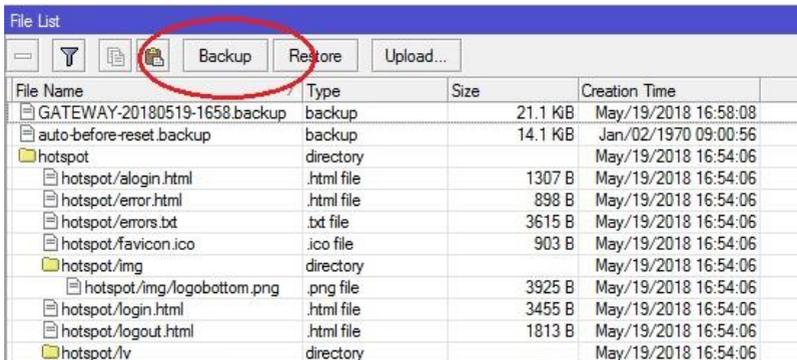
Backup

Proses backup ini sangat berguna, mana kala Anda ingin melakukan proses penggantian router. Karena konfigurasi sudah di-backup, maka saat akan menggunakan router yang baru, tidak perlu lagi melakukan proses konfigurasi dari awal. Tentunya akan sangat menghemat waktu dan tenaga. Begitu pula untuk meng-antisipasi jika suatu saat router yang digunakan bermasalah atau *crash*. Jika suatu saat router mengalami *crash* dan tidak dapat diakses lagi, maka Anda sudah memiliki semua konfigurasi yang sudah pernah dilakukan, sehingga akan mudah menggunakannya kembali pada router yang baru.

Untuk melakukan proses backup, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > system backup save password=123456
Saving system configuration
Configuration backup saved
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Files** → tombol **Backup**, seperti pada gambar berikut ini.



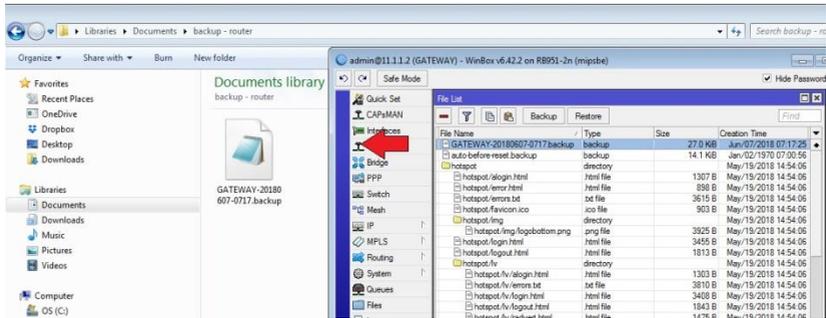
Gambar 9.1
Proses Backup

Setelah proses backup selesai, maka akan dihasilkan sebuah file dengan ekstensi .backup, yang dapat dilihat dengan menggunakan berikut ini.

```
[admin@GATEWAY] > file print
# NAME                                     TYPE                SIZE CREATION-TIME
0 hotspot/redirect.html                  .html file           318 may/19/2018
1 hotspot/xml/alogin.html                 .html file           821 may/19/2018
2 hotspot/xml/error.html                  .html file           416 may/19/2018
3 hotspot/xml/flogout.html                .html file           361 may/19/2018
4 hotspot                                 directory            may/19/2018
5 hotspot/xml/logout.html                 .html file           359 may/19/2018
6 hotspot/error.html                      .html file           898 may/19/2018
7 hotspot/errors.txt                       .txt file           3615 may/19/2018
8 hotspot/img                             directory            may/19/2018
9 hotspot/logout.html                     .html file           1813 may/19/2018
10 hotspot/lv/login.html                   .html file           3408 may/19/2018
11 GATEWAY-20180519-1658.backup            backup               21.1KiB may/19/2018
12 skins                                   directory            jan/01/1970
13 hotspot/radvert.html                    .html file           1509 may/19/2018
14 hotspot/rlogin.html                     .html file           850 may/19/2018
15 hotspot/xml/WISPAccessGatewayP.xsd     file                 4251 may/19/2018
```

File backup tersebut akan berisi semua konfigurasi yang sudah dilakukan. Yang terpenting dalam melakukan backup adalah parameter *password*. Dengan menggunakan parameter *password*, maka file backup tersebut tidak akan mudah digunakan oleh orang lain.

Secara default, file backup disimpan pada disk dari Router MikroTik. Untuk menjaga hal-hal yang tidak diinginkan, seperti kondisi disk yang rusak, maka sebaiknya file tersebut juga disimpan di laptop atau tempat penyimpanan yang lain. Untuk menyimpannya ke dalam laptop, Anda tinggal melakukan *drag n drop* ke desktop laptop atau pun ke sebuah direktori pada laptop Anda, seperti pada gambar berikut ini.

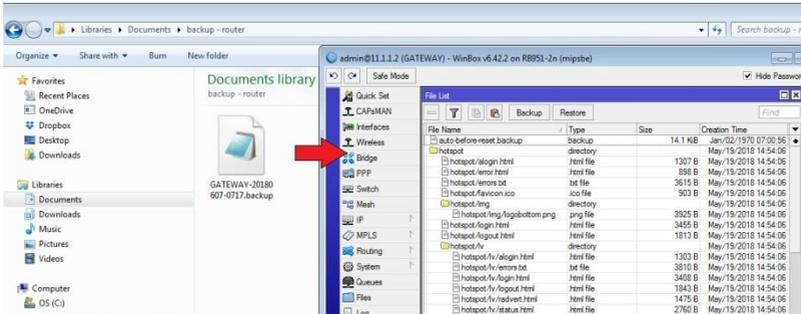


Gambar 9.2
Drag n drop ke laptop

Sebagai catatan penting, halaman login yang digunakan oleh Hotspot Server tidak akan dibackup oleh proses backup konfigurasi. Untuk melakukan backup halaman login, Anda tinggal melakukan *drag n drop* terhadap direktori *hotspot* ke laptop Anda.

Restore

Proses restore adalah proses mengembalikan konfigurasi-konfigurasi yang sudah disimpan pada proses backup. Sebelum proses restore dilakukan harus dipastikan bahwa file backup yang akan digunakan sudah ada di dalam disk Router MikroTik. Jika file backupnya masih berada di laptop, maka dapat dilakukan *drag n drop* ke dalam menu **Files**, seperti pada gambar berikut ini.

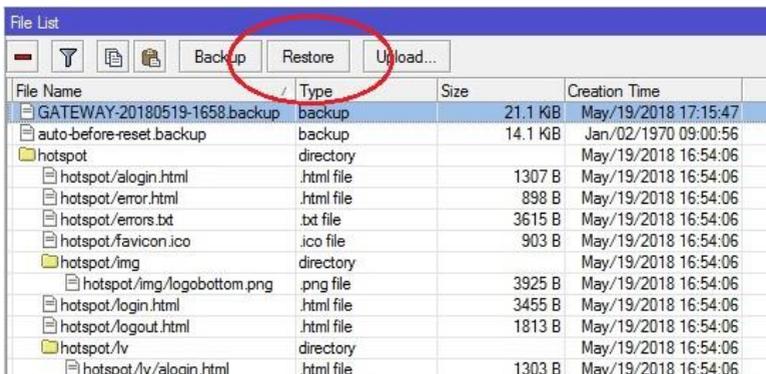


Gambar 9.3
Drag n drop file backup

Untuk melakukan proses restore, perintah berikut ini dapat digunakan, jika file tersebut memiliki password saat proses backup, maka proses restore akan meminta password tersebut.

```
[admin@GATEWAY] > system backup load
name=GATEWAY-20180519-1658.backup password=123456
Restore and reboot? [y/N]:y
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah menu **Files** → memilih file backup, kemudian melakukan klik tombol **Restore**, seperti pada gambar berikut ini.



Gambar 9.4
Proses Restore

Setelah proses restore dilakukan, maka Router MikroTik akan melakukan reboot atau restart. Sebagai catatan lagi, jika proses backup dan restore dilakukan antara dua jenis router yang berbeda, maka terkadang Anda harus melakukan penyesuaian urutan interface. Sebagai contoh, Anda harus melakukan penyusunan interface kembali jika proses backup dilakukan pada RouterBoard 951, dan file backup tersebut akan di-restore pada RouterBoard 1100.

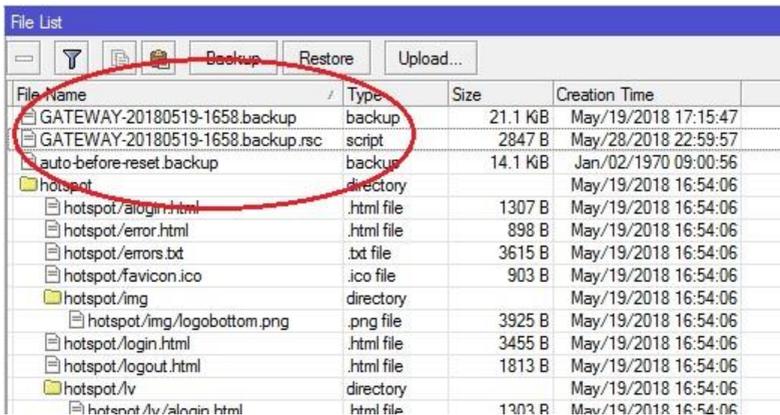
Export

Untuk mencegah proses penyusunan kembali interface pada saat proses restore, maka dapat digunakan fitur **export** pada saat akan melakukan backup. Kelebihan menggunakan **export** adalah file hasil backup juga akan bisa dilihat dengan menggunakan Notepad pada komputer Windows. Dengan demikian baris-baris konfigurasi yang pernah dilakukan akan terlihat dengan jelas.

Asumsi yang digunakan pada pembahasan ini adalah proses backup sudah dilakukan dan file backup yang dihasilkan adalah *GATEWAY-20180519-1658.backup*. Untuk melakukan proses export, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > export file=GATEWAY-20180519-1658.backup
```

Setelah proses export akan dihasilkan sebuah file dengan ekstensi .rsc. seperti terlihat pada gambar berikut ini.

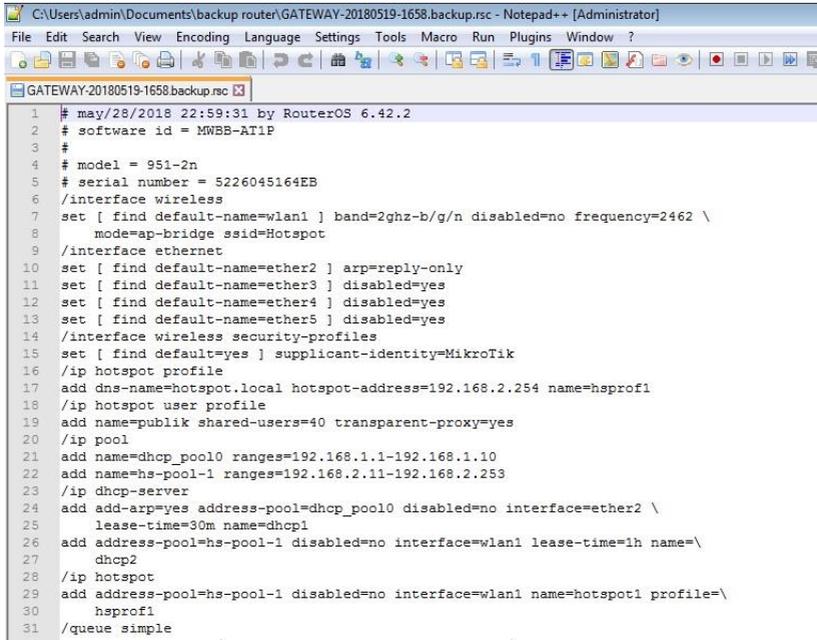


The screenshot shows a 'File List' window with a table of files. A red circle highlights the file 'GATEWAY-20180519-1658.backup.rsc'. The table has columns for File Name, Type, Size, and Creation Time.

File Name	Type	Size	Creation Time
GATEWAY-20180519-1658.backup	backup	21.1 KiB	May/19/2018 17:15:47
GATEWAY-20180519-1658.backup.rsc	script	2847 B	May/28/2018 22:59:57
auto-before-reset.backup	backup	14.1 KiB	Jan/02/1970 09:00:56
hotspot	directory		May/19/2018 16:54:06
hotspot/alogin.html	.html file	1307 B	May/19/2018 16:54:06
hotspot/error.html	.html file	898 B	May/19/2018 16:54:06
hotspot/errors.txt	.txt file	3615 B	May/19/2018 16:54:06
hotspot/favicon.ico	.ico file	903 B	May/19/2018 16:54:06
hotspot/img	directory		May/19/2018 16:54:06
hotspot/img/logobottom.png	.png file	3925 B	May/19/2018 16:54:06
hotspot/login.html	.html file	3455 B	May/19/2018 16:54:06
hotspot/logout.html	.html file	1813 B	May/19/2018 16:54:06
hotspot/iv	directory		May/19/2018 16:54:06
hotspot/iv/alogin.html	html file	1307 B	May/19/2018 16:54:06

Gambar 9.5
File hasil export

File tersebut dapat dipindahkan ke laptop dengan proses *drag n drop*. Dan setelah berada di laptop, file tersebut dapat dibuka dengan menggunakan aplikasi **Notepad++** atau **Wordpad**, seperti terlihat pada gambar berikut ini.



```
1 # may/28/2018 22:59:31 by RouterOS 6.42.2
2 # software id = MWBB-AT1P
3 #
4 # model = 951-2n
5 # serial number = 5226045164EB
6 /interface wireless
7 set [ find default-name=wlan1 ] band=2ghz-b/g/n disabled=no frequency=2462 \
8     mode=ap-bridge ssid=Hotspot
9 /interface ethernet
10 set [ find default-name=ether2 ] arp=reply-only
11 set [ find default-name=ether3 ] disabled=yes
12 set [ find default-name=ether4 ] disabled=yes
13 set [ find default-name=ether5 ] disabled=yes
14 /interface wireless security-profiles
15 set [ find default=yes ] supplicant-identity=MikroTik
16 /ip hotspot profile
17 add dns-name=hotspot.local hotspot-address=192.168.2.254 name=hsprof1
18 /ip hotspot user profile
19 add name=publik shared-users=40 transparent-proxy=yes
20 /ip pool
21 add name=dhcp_pool0 ranges=192.168.1.1-192.168.1.10
22 add name=hs-pool-1 ranges=192.168.2.11-192.168.2.253
23 /ip dhcp-server
24 add add-arp=yes address-pool=dhcp_pool0 disabled=no interface=ether2 \
25     lease-time=30m name=dhcp1
26 add address-pool=hs-pool-1 disabled=no interface=wlan1 lease-time=1h name=\
27     dhcp2
28 /ip hotspot
29 add address-pool=hs-pool-1 disabled=no interface=wlan1 name=hotspot1 profile=\
30     hsprof1
31 /queue simple
```

Gambar 9.6
File konfigurasi dibuka dengan Notepad++

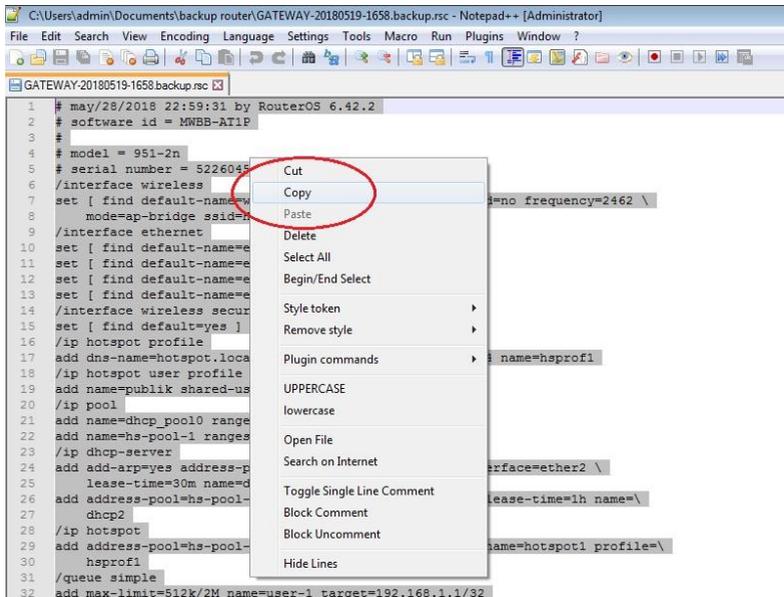
Dari gambar 9.6, terlihat bahwa semua detail konfigurasi dapat dengan mudah terbaca. Konfigurasi-konfigurasi tersebut dapat pula Anda gunakan untuk melakukan restore konfigurasi.

Untuk melakukan proses restore dengan menggunakan file hasil export, langkah-langkah yang perlu dilakukan dapat dijabarkan sebagai berikut.

1. Sebaiknya dipastikan bahwa Router yang digunakan tidak memiliki konfigurasi apapun. Anda dapat melakukan proses reset configuration untuk mengosongkan semua konfigurasi dengan menggunakan perintah berikut ini.

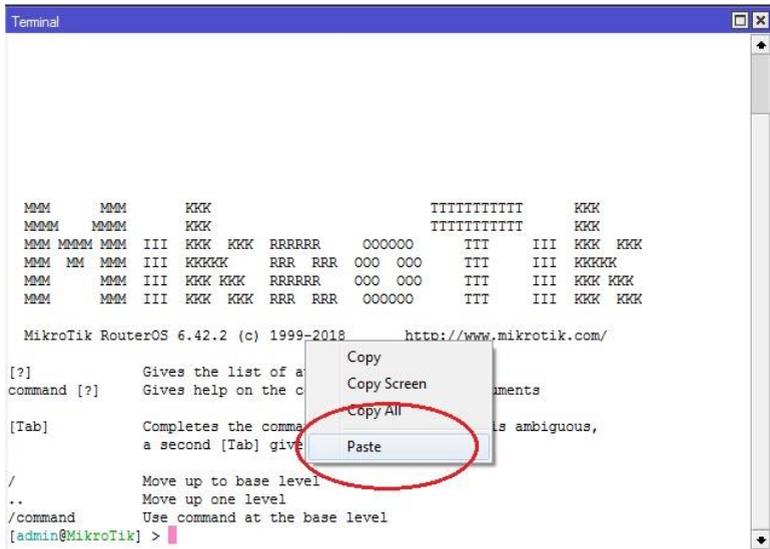
```
[admin@GATEWAY] > system reset-configuration no-default=yes
```

2. Setelah proses reset selesai, maka Anda dapat membuka file hasil export dengan menggunakan Notepad++ kemudian melakukan copy terhadap semua baris konfigurasi yang ada pada Notepad++. Anda bisa menggunakan cara [Control A] untuk memilih semua baris konfigurasi dan [Control C] untuk melakukan copy konfigurasi pada Notepad++.



Gambar 9.7
Proses Copy konfigurasi pada Notepad++

3. Setelah itu, proses restore dapat dilanjutkan dengan membuka menu **New Terminal** pada WinBox Router MikroTik, melakukan klik kanan dan melakukan paste, seperti terlihat pada gambar berikut ini.



Gambar 9.8
Proses Restore pada menu New Terminal

4. Setelah langkah paste konfigurasi dilakukan pada **New Terminal**, maka proses restore telah selesai, dan Router MikroTik siap digunakan dengan konfigurasi yang baru. Untuk proses restore seperti ini, tidak perlu dilakukan prosedur reboot pada Router MikroTik.

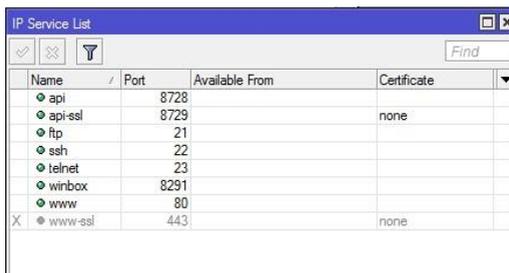
Manajemen Service

Selain tugas utama untuk menghubungkan jaringan lokal ke Internet, Router MikroTik juga menjalankan beberapa service untuk menunjang tugas utama tersebut. Sebagai contoh, Router MikroTik harus menjalankan service WinBox, agar Anda dapat melakukan konfigurasi dengan menggunakan WinBox. Juga menjalankan service web, sehingga Anda juga bisa melakukan konfigurasi dengan menggunakan web browser.

Secara default, Router MikroTik akan langsung menjalankan beberapa service. Untuk melihat service tersebut, dapat digunakan perintah berikut ini.

```
[admin@GATEWAY] > ip service print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS  CERTIFICATE
0  telnet    23
1  ftp       21
2  www       80
3  ssh       22
4  XI www-ssl  443      none
5  api       8728
6  winbox    8291
7  api-ssl   8729      none
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Services**, seperti terlihat pada gambar berikut ini.



Gambar 9.9
Service yang dijalankan Router MikroTik

Untuk meningkatkan keamanan dari Router MikroTik itu sendiri, maka service-service yang tidak dibutuhkan umumnya akan dinonaktifkan (di disable). Sebagai contoh, service telnet dan ssh umumnya dapat digunakan oleh pihak yang tidak bertanggungjawab untuk mencoba login ke dalam sistem Router MikroTik. Sebagai contoh, jika ingin men-disable beberapa service, seperti service ssh, telnet dan ftp, maka perintah berikut ini dapat digunakan.

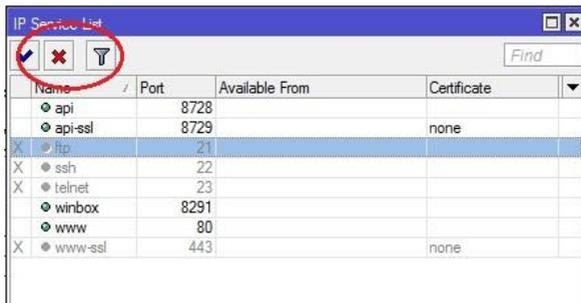
```
[admin@GATEWAY] > ip service disable ftp

[admin@GATEWAY] > ip service disable ssh

[admin@GATEWAY] > ip service disable telnet

[admin@GATEWAY] > ip service print
Flags: X - disabled, I - invalid
#  NAME          PORT ADDRESS  CERTIFICATE
0  XI telnet      23
1  XI ftp         21
2  www           80
3  XI ssh        22
4  XI www-ssl    443          none
5  api           8728
6  winbox       8291
7  api-ssl      8729          none
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **IP → Services**, memilih service yang akan di-disable, kemudian meng-klik tombol **Disable**, seperti pada gambar berikut ini.



Gambar 9.10
Meng-disable beberapa service

Untuk service yang masih dibutuhkan, beberapa Administrator melakukan pergantian nomor port. Sebagai contoh, port default untuk service WinBox adalah 8291. Anda bisa saja menggantiknya ke port 8888, sehingga tidak semua orang mengetahui port yang digunakan untuk melakukan remote login ke dalam Router MikroTik. Sebagai contoh, jika ingin mengganti nomor port WinBox, ke port 8888, maka perintah berikut ini dapat digunakan.

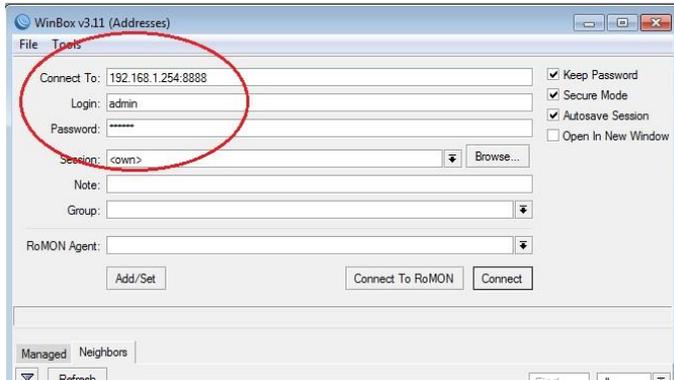
```
[admin@GATEWAY] > ip service set winbox port=8888
```

Dengan menggunakan WinBox, Anda cukup memilih service WinBox, meng-klik 2x service tersebut untuk mengganti port-nya seperti pada gambar berikut ini.

Gambar 9.11
Mengganti port WinBox



Karena port WinBox sudah tidak menggunakan nilai default-nya, maka saat akan melakukan remote dengan WinBox, Anda harus menambahkan port 8888 sesudah alamat dari Router MikroTik itu sendiri, seperti terlihat pada gambar berikut ini.



Gambar 9.12
Mengakses Router MikroTik dengan port 8888

Manajemen System

Untuk menjalankan tugasnya sebagai router maupun tugas tambahan lainnya, Router MikroTik disusun dari beberapa Package System atau paket sistem.

Sebagai contoh, agar bisa menjadi Access Point untuk melayani jaringan wireless, Router MikroTik harus memiliki package wireless. Package inilah yang akan mengenali interface wireless, serta menampilkan menu konfigurasi wireless. Walaupun Router MikroTik memiliki interface wireless, namun jika package wireless tidak terinstall pada router tersebut, Anda tidak akan bisa melakukan konfigurasi wireless. Dan tentunya interface wireless tadi tidak bisa digunakan untuk menjadi Access Point.

Untuk melihat package apa saja yang terinstall pada sebuah Router MikroTik, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > system package print
Flags: X - disabled
#  NAME                VERSION  SCHEDULED
0  routeros-mipsbe     6.42.2
1  system              6.42.2
2  X ipv6              6.42.2
3  wireless            6.42.2
4  hotspot             6.42.2
5  dhcp                6.42.2
6  mpls                6.42.2
7  routing             6.42.2
8  ppp                 6.42.2
9  security            6.42.2
10 advanced-tools     6.42.2
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **System → Packages**, seperti terlihat pada gambar berikut ini.

Name	Version	Build Time	Scheduled
routeros-mipsbe	6.42.2	May/17/2018 09:20:36	
advanced-tools	6.42.2	May/17/2018 09:20:36	
dhcp	6.42.2	May/17/2018 09:20:36	
hotspot	6.42.2	May/17/2018 09:20:36	
ipv6	6.42.2	May/17/2018 09:20:36	
mpls	6.42.2	May/17/2018 09:20:36	
ppp	6.42.2	May/17/2018 09:20:36	
routing	6.42.2	May/17/2018 09:20:36	
security	6.42.2	May/17/2018 09:20:36	
system	6.42.2	May/17/2018 09:20:36	
wireless	6.42.2	May/17/2018 09:20:36	

Gambar 9.13
Sistem Package pada Router MikroTik

Dari gambar 9.13, dapat dilihat package apa saja yang terinstall pada sebuah Router MikroTik. Terlihat pula package apa saja yang diaktifkan atau tidak diaktifkan.

Enable/Disable Package

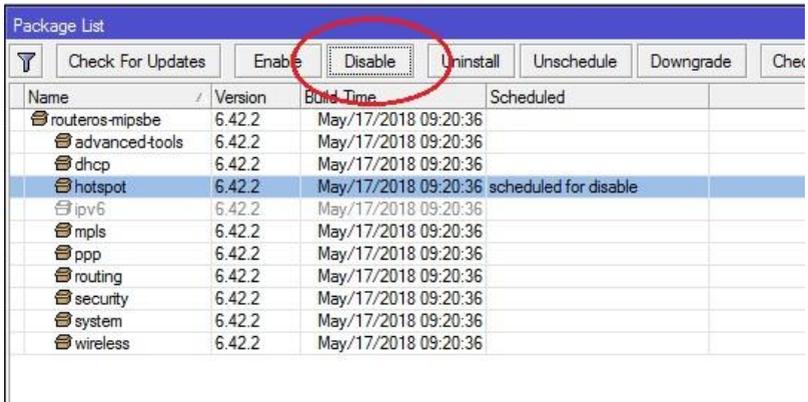
Untuk menghemat penggunaan resource dari router, beberapa package yang tidak digunakan bisa saja dinonaktifkan atau di-disable. Misalnya saja, jika Router MikroTik tidak akan menjalankan Hotspot Server, maka package *hotspot*, bisa saja di-disable.

Sebagai contoh, untuk meng-disable package *hotspot*, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > system package disable hotspot

[admin@GATEWAY] > system package print
Flags: X - disabled
#  NAME                VERSION  SCHEDULED
0  routeros-mipsbe     6.42.2
1  system              6.42.2
2  X ipv6              6.42.2
3  wireless            6.42.2
4  hotspot             6.42.2  scheduled for disable
5  dhcp                6.42.2
6  mpls                6.42.2
7  routing             6.42.2
8  ppp                 6.42.2
9  security            6.42.2
10 advanced-tools     6.42.2
```

Dengan menggunakan WinBox, Anda tinggal memilih package yang diinginkan, untuk kemudian memilih tombol **Disable**, seperti terlihat pada gambar berikut ini.



Gambar 9.14
Tombol Disable package

Untuk benar-benar menonaktifkan package tadi, perlu dilakukan prosedur restart terhadap Router Mikrotik.

Jika suatu saat, package hotspot perlu diaktifkan kembali, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > system package enable hotspot
```

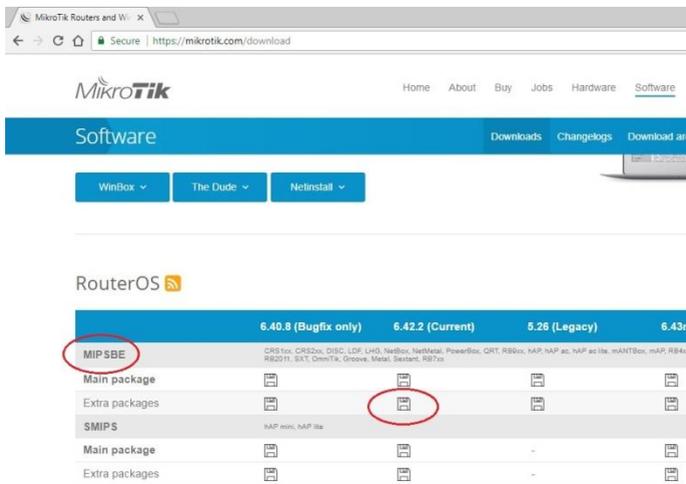
Pada WinBox, Anda hanya perlu memilih package yang diinginkan untuk kemudian melakukan klik tombol **Enable** jika suatu saat ada package yang perlu diaktifkan kembali.

Download Package

Untuk melakukan manajemen package, seperti menambahkan atau mengurangi package, maka Anda harus men-download package yang diinginkan. Package-package dikemas dalam bentuk sebuah

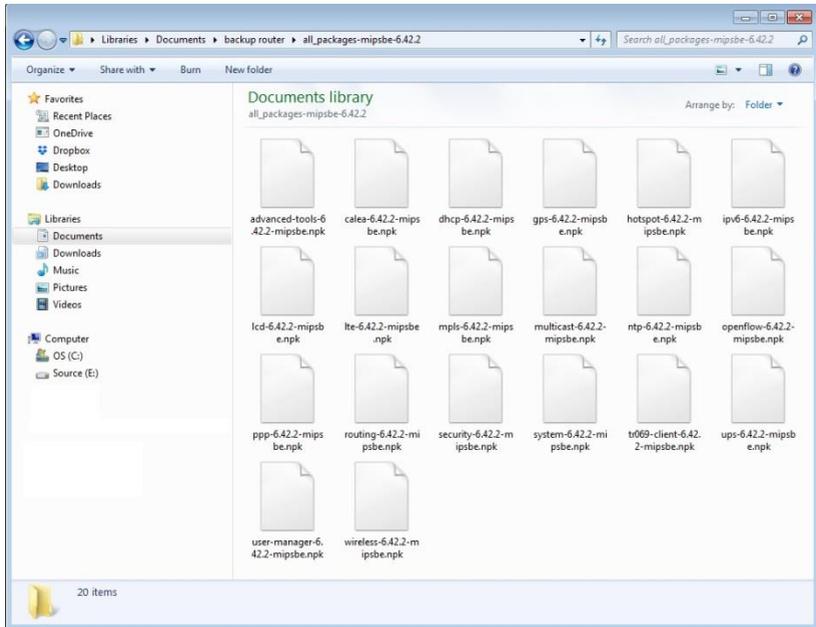
file dengan ekstensi .zip. Anda dapat meng-downloadnya pada alamat <https://mikrotik.com/download>.

Yang harus diperhatikan pada saat melakukan download adalah kecocokan antara jenis router yang digunakan dengan jenis package. Sebagai contoh, buku ini menggunakan Router MikroTik RB951-2n yang memiliki arsitektur CPU Mipsbe. Karena menggunakan arsitektur CPU Mipsbe, maka file package yang harus di-download juga adalah file yang ditujukan untuk arsitektur Mipsbe, seperti terlihat pada gambar berikut ini.



Gambar 9.15
Extra Package untuk menambahkan system package

Setelah file extra packages tersebut berhasil di-download, untuk melihat berbagai package yang ada, file tersebut dapat di-unzip dengan menggunakan aplikasi seperti WinZip atau WinRAR. Hasil dari ekstrak atau proses unzip dari file extra packages tersebut akan memperlihatkan beberapa file package yang berekstensi .npk.



Gambar 9.16
Kumpulan file package untuk arsitektur Mipsbe

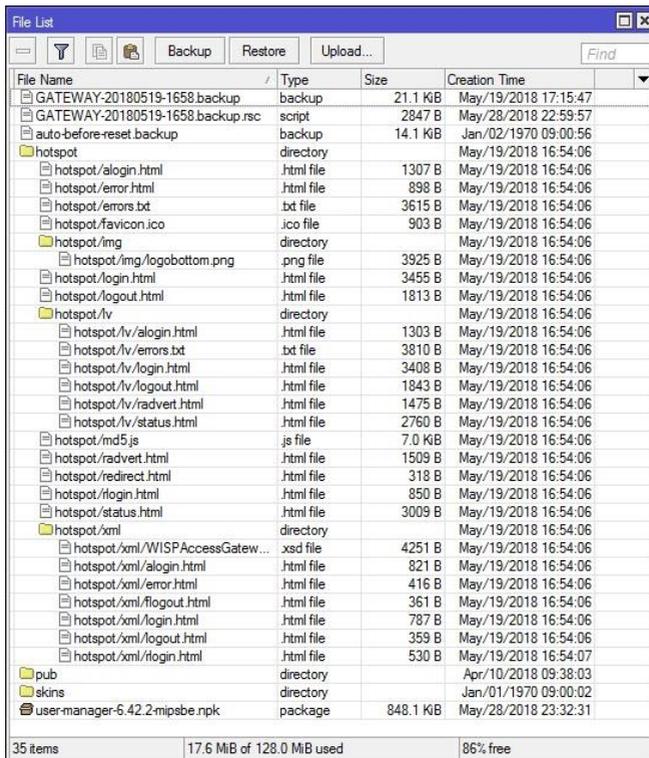
Dari gambar 9.16, terlihat beberapa file dengan ekstensi .npk. File-file inilah yang nantinya dapat Anda gunakan untuk menambahkan package pada Router MikroTik.

Menambahkan Package

Pada bagian ini akan dibahas bagaimana menambahkan package ke dalam Router MikroTik. Asumsi yang digunakan adalah Anda sudah melakukan download file extra packages dan meng-ekstraknya seperti pada pembahasan sebelumnya.

Adapun contoh penambahan package yang akan dilakukan adalah menambahkan package User Manager. Paket User Manager ini digunakan untuk menunjang kinerja dari Hotspot Server.

Penambahan package User Manager dapat dimulai dengan mengupload file **user-manager-6.42.2-mipsbe.npk** ke menu **Files** Router MikroTik. Untuk melakukannya, Anda cukup melakukan *drag n drop* ke menu **Files** yang ada pada WinBox. Jika proses upload telah selesai, maka menu **Files** akan terlihat seperti gambar berikut ini.



Gambar 9.17
File instalasi User Manager pada menu Files

Setelah dipastikan benar file package User Manager berada pada menu **Files**, tahapan instalasi bisa dijalankan dengan melakukan

restart terhadap Router MikroTik. Perintah untuk melakukan restart adalah sebagai berikut.

```
[admin@GATEWAY] > system reboot  
Reboot, yes? [y/N]:  
y  
system will reboot shortly
```

Setelah proses reboot selesai, package User Manager seharusnya sudah terinstall pada Router GW. Untuk memastikannya perintah berikut ini dapat digunakan.

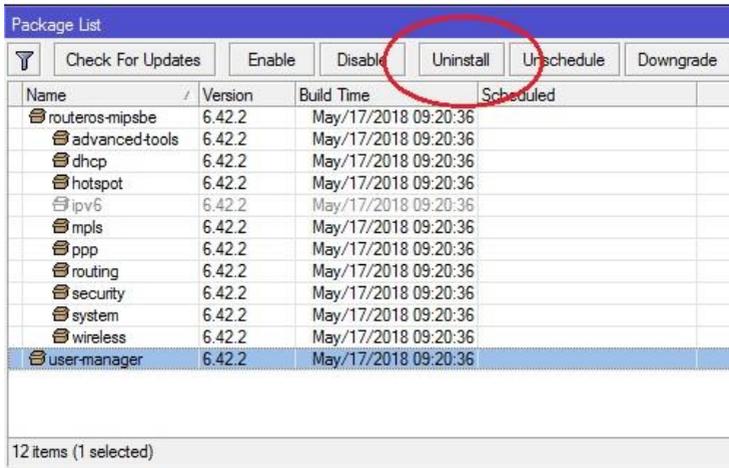
```
[admin@GATEWAY] > system package print  
Flags: X - disabled  
# NAME VERSION SCHEDULED  
0 user-manager 6.42.2  
1 routeros-mipsbe 6.42.2  
2 system 6.42.2  
3 X ipv6 6.42.2  
4 wireless 6.42.2  
5 hotspot 6.42.2  
6 dhcp 6.42.2  
7 mpls 6.42.2  
8 routing 6.42.2  
9 ppp 6.42.2  
10 security 6.42.2  
11 advanced-tools 6.42.2
```

Menghapus Package

Menghapus package sistem yang tidak dibutuhkan akan bisa menghemat resource router, terutama penghematan terhadap penggunaan disk dan CPU. Sebagai contoh, jika package wireless ternyata tidak dibutuhkan, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > system package uninstall user-manager
```

Dengan menggunakan WinBox, Anda dapat menggunakan tombol **Uninstall**, seperti terlihat pada gambar berikut ini.



Gambar 9.18
Menghapus package yang tidak dibutuhkan

Setelah melakukan perintah penghapusan seperti pada uraian tadi, Anda harus melakukan tahapan restart atau reboot router untuk menuntaskan tahapan penghapusan tadi.

Upgrade RouterOS

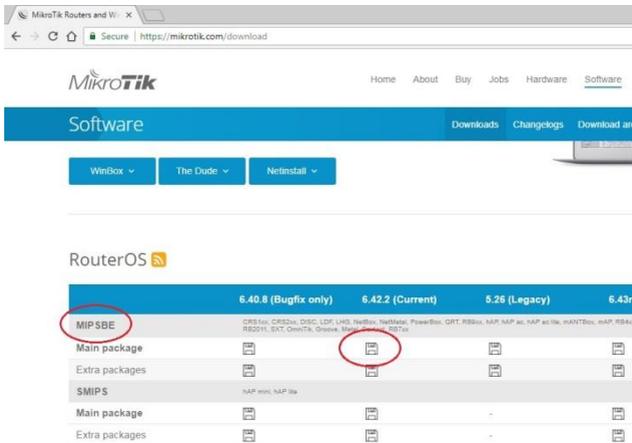
Untuk meningkatkan kehandalan dan kestabilan, RouterOS yang merupakan sistem operasi Router MikroTik sangat disarankan untuk selalu di-update. Dengan melakukan update, maka akan terjadi pembaruan terhadap sistem operasi router beserta packages sistem yang digunakan. Ini sangat berguna, karena dengan proses update, bug atau kegagalan sistem dari versi RouterOS sebelumnya akan selalu diperbaiki pada versi terbaru. Begitu juga dengan fitur-fitur terbaru, versi RouterOS yang lebih baru umumnya akan dilengkapi dengan fitur-fitur terbaru pula.

Yang perlu diperhatikan saat melakukan proses upgrade adalah kesesuaian file yang akan digunakan untuk upgrade dengan jenis CPU yang digunakan. Sebagai contoh, pada buku ini digunakan RouterBoard RB951-2n yang menggunakan arsitektur CPU Mipsbe, sehingga Anda harus menggunakan file upgrade RouterOS untuk arsitektur Mipsbe pula. Selain itu, yang perlu diperhatikan bahwa file upgrade RouterOS adalah file dengan ekstensi .npk

Asumsi yang digunakan pada prosedur ini adalah RouterOS yang masih menggunakan RouterOS versi 6.39. Untuk melakukan proses upgrade (misalnya ke versi 6.42.2) tahapannya dapat diuraikan seperti berikut ini.

1. Melakukan download file upgrade RouterOS pada halaman <https://mikrotik.com/download>. Untuk contoh tahapan ini, file yang akan digunakan adalah **routeros-mipsbe-6.42.2.npk**, seperti terlihat pada gambar berikut ini.

Gambar File

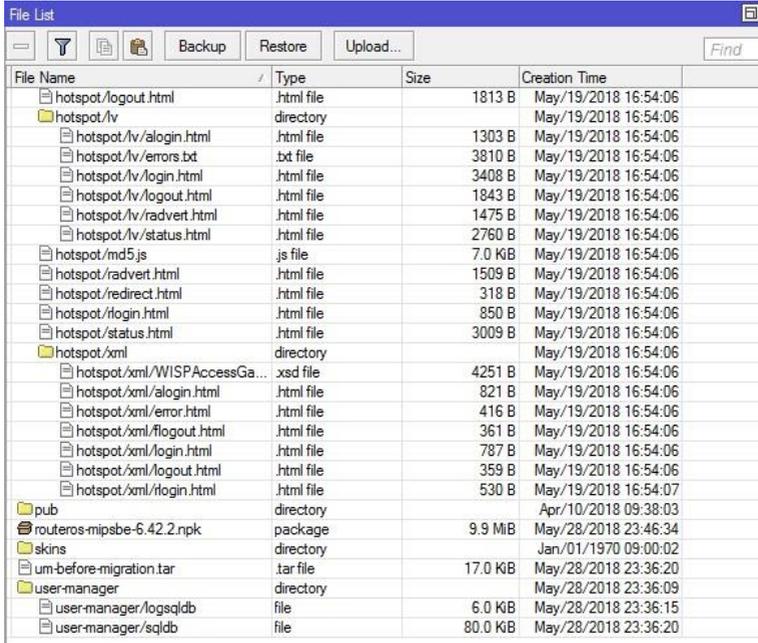


9.19

upgrade RouterOS untuk Mipsbe

Setelah proses download selesai, maka akan didapatkan file dengan ekstensi .npk pada laptop Anda.

- Langkah kedua adalah memindahkan file tersebut ke disk Router MikroTik. Untuk prosedur ini, Anda dapat melakukannya dengan *drag n drop* ke menu **Files**, seperti terlihat pada gambar berikut ini.



Gambar 9.20
File Main Package di menu **Files**

- Jika file **routers-mipsbe-6.42.2.npk** tersebut sudah berada di menu **Files**, maka dapat dilakukan proses reboot atau restart dengan menggunakan perintah berikut ini.

```
[admin@GATEWAY] > system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
```

- Setelah proses reboot selesai, maka seharusnya versi RouterOS akan menjadi versi terbaru sesuai versi file .npk yang digunakan.

Tentunya pemeriksaan versi RouterOS dapat dilakukan dengan menggunakan perintah berikut ini.

```
[admin@GATEWAY] > system resource print
    uptime: 1m33s
    version: 6.42.2 (stable)
    build-time: Oct/31/2017 13:05:15
    free-memory: 9.6MiB
    total-memory: 32.0MiB
    cpu: MIPS 24Kc V7.4
    cpu-count: 1
    cpu-frequency: 360MHz
    cpu-load: 10%
    free-hdd-space: 47.9MiB
    total-hdd-space: 64.0MiB
    write-sect-since-reboot: 180
    write-sect-total: 1090358
    bad-blocks: 2.3%
    architecture-name: mipsbe
    board-name: RB951-2n
    platform: MikroTik
```

Pada proses upgrade ini, yang perlu diperhatikan adalah keberadaan file .npk pada menu **Files**. Jika keseluruhan proses upgrade berhasil, maka file upgrade tadi tidak akan terlihat lagi pada menu **Files**.

End of Chapter

Bab 10

Monitoring

Setelah membangun jaringan dengan Router MikroTik, melakukan manajemen jaringan serta melakukan manajemen terhadap router, maka pekerjaan terakhir yang harus dilakukan oleh seorang Administrator jaringan adalah melakukan tugas monitoring. Monitoring ini berguna untuk mengetahui apa saja yang terjadi dengan jaringan maupun apa yang terjadi dengan Router itu sendiri. Dari hasil monitoring, akan didapat hal-hal penting yang bisa saja digunakan untuk perbaikan konfigurasi, pemeliharaan router atau pun kebutuhan penambahan alokasi bandwidth.

Untuk tahapan awal, pekerjaan monitoring hanya dilakukan dengan memanfaatkan fitur-fitur yang ada di dalam Router MikroTik itu sendiri. Untuk jaringan dengan skala kecil dan sederhana, maka penggunaan fitur-fitur tersebut sudah dapat diandalkan. Namun, bila suatu saat akan mengelola jaringan yang lebih besar, maka penggunaan Network Management System (NMS) akan lebih disarankan.

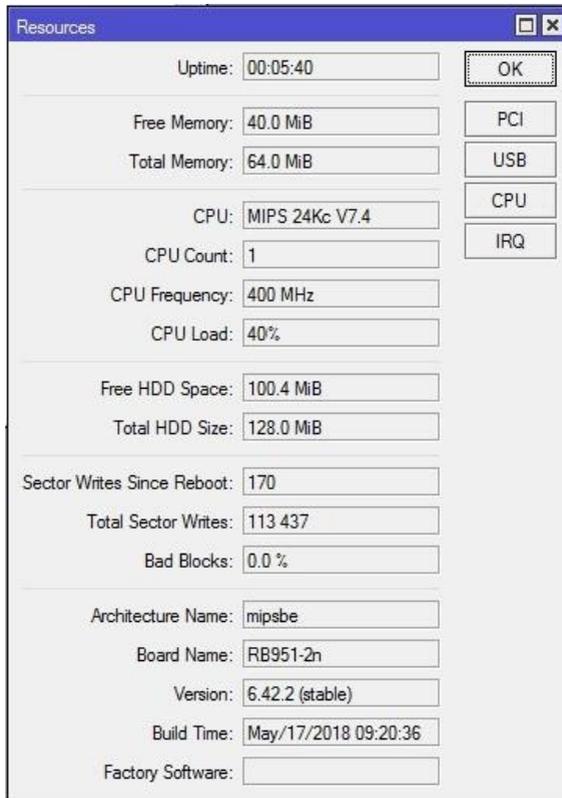
Monitoring Hardware

Yang paling pertama dan sangat penting adalah melakukan pemantauan hardware dari sebuah router. Kondisi dan pemakaian kapasitas pemakaian hardware akan sangat menentukan performa router di dalam jaringan. Yang pada akhirnya, performa router juga akan menentukan performa dari jaringan yang Anda bangun. Kondisi hardware yang baik tentu akan menghasilkan kondisi jaringan yang baik pula.

Kondisi hardware yang sangat penting untuk diawasi adalah penggunaan processor (CPU), memori, maupun hard disk/disk/chip yang digunakan untuk menyimpan RouterOS dan konfigurasi. Untuk melakukan monitoring penggunaan resource tadi, perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > system resource print
    uptime: 4m35s
    version: 6.42.2 (stable)
    build-time: May/17/2018 09:20:36
    free-memory: 39.7MiB
    total-memory: 64.0MiB
    cpu: MIPS 24Kc V7.4
    cpu-count: 1
    cpu-frequency: 400MHz
    cpu-load: 40%
    free-hdd-space: 100.4MiB
    total-hdd-space: 128.0MiB
    write-sect-since-reboot: 170
    write-sect-total: 113437
    bad-blocks: 0%
    architecture-name: mipsbe
    board-name: RB951-2n
    platform: MikroTik
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **System → Resource**, seperti pada gambar berikut ini.



Gambar 10.1
Resource Hardware dari RouterBoard 951-2n

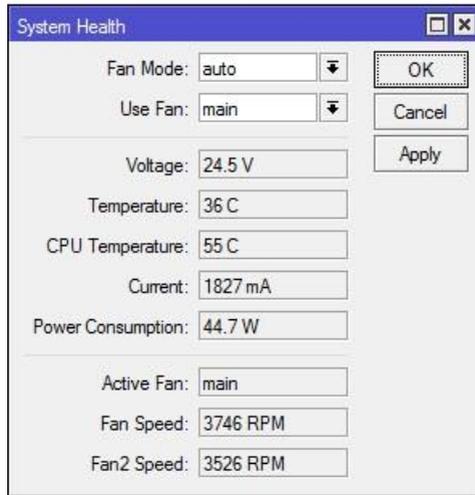
Dari uraian dan gambar 10.1, terlihat kondisi dari hardware RouterBoard 951-2n. Anda dapat melihat berapa lama router tersebut telah dihidupkan (*uptime*), penggunaan memori (*free-memory* dan *total-memory*), jumlah CPU (*cpu-count*), berapa persen kapasitas CPU sudah digunakan (*cpu-load*) dan berapa kapasitas disk router (*free-hdd-space* dan *total-hdd-space*). Juga terlihat arsitektur dari router ini adalah *mipsbe* dan sedang menggunakan RouterOS versi 6.42.2

Saat melakukan monitoring resource ini, kapasitas hardware yang selalu menjadi perhatian adalah presentasi penggunaan CPU (*cpu-load*). Jika nilai dari *cpu-load* sudah mendekati 100%, maka itu menandakan kapasitas Router MikroTik Anda sudah tidak mencukupi untuk melakukan pekerjaan pengelolaan jaringan. Hal ini juga merupakan peringatan, agar Anda sudah harus mempertimbangkan untuk menggunakan Router MikroTik dengan kapasitas CPU yang lebih besar. Kalaupun masih ingin mempertahankan router yang bersangkutan, Anda harus mulai mengurangi konfigurasi dan fitur-fitur yang dijalankan oleh router tersebut, atau bahkan mengurangi bandwidth yang digunakan oleh jaringan Anda ☺.

Beberapa seri Router MikroTik bisa melakukan monitoring terhadap suhu atau temperature dari CPU. Sebagai contoh, uraian berikut ini adalah perintah yang diberikan kepada Router MikroTik seri Cloud Core Router (CCR).

```
[admin@GATEWAY > system health print
      fan-mode: auto
      use-fan: main
      active-fan: main
      cpu-overtemp-check: yes
      cpu-overtemp-threshold: 100C
      cpu-overtemp-startup-delay: 1m
      voltage: 24.5V
      current: 1825mA
      temperature: 36C
      cpu-temperature: 55C
      power-consumption: 44.7W
      fan1-speed: 3530RPM
      fan2-speed: 3310RPM
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **System → Health**, seperti gambar berikut ini.



Gambar 10.2
System Health dari Router seri CCR

Dari uraian tadi dan gambar 10.2, Anda akan mendapati beberapa informasi penting seperti penggunaan tegangan listrik, temperature (suhu) maupun kecepatan kipas pendingin yang digunakan oleh Router MikroTik.

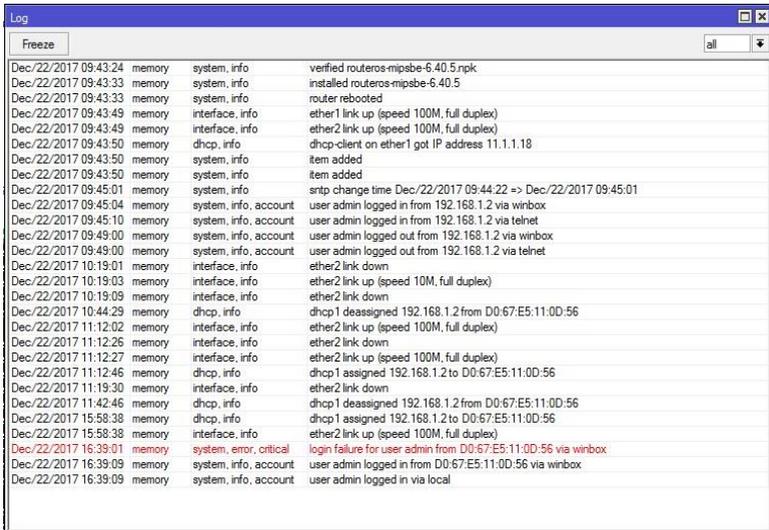
Membaca Log

Tugas monitoring yang juga sangat penting adalah membaca Log dari Router MikroTik. Log ini akan menyimpan berbagai informasi penting yang terjadi pada Router MikroTik. Mulai dari percobaan login yang gagal dari user yang ingin melakukan konfigurasi, catatan penambahan konfigurasi, ada tidaknya user yang menggunakan DHCP Server, status dari setiap interface dan banyak informasi lainnya yang ditampilkan oleh fitur Log ini.

Untuk melihat Log, perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > log print
09:43:24 system,info verified routeros-mipsbe-6.40.5.npk
09:43:33 system,info installed routeros-mipsbe-6.40.5
09:43:33 system,info router rebooted
09:43:49 interface,info ether1 link up (speed 100M, full duplex)
09:43:49 interface,info ether2 link up (speed 100M, full duplex)
09:43:50 dhcp,info dhcp-client on ether1 got IP address 11.1.1.18
09:43:50 system,info item added
09:43:50 system,info item added
09:45:01 system,info sntp change time Dec/22/2017 09:44:22 => Dec/22
09:45:04 system,info,account user admin logged in from 192.168.1.2 v
09:45:10 system,info,account user admin logged in from 192.168.1.2 v
09:49:00 system,info,account user admin logged out from 192.168.1.2
09:49:00 system,info,account user admin logged out from 192.168.1.2
10:19:01 interface,info ether2 link down
10:19:03 interface,info ether2 link up (speed 10M, full duplex)
10:19:09 interface,info ether2 link down
10:44:29 dhcp,info dhcp1 deassigned 192.168.1.2 from D0:67:E5:11:0D:
11:12:02 interface,info ether2 link up (speed 100M, full duplex)
11:12:26 interface,info ether2 link down
11:12:27 interface,info ether2 link up (speed 100M, full duplex)
11:12:46 dhcp,info dhcp1 assigned 192.168.1.2 to D0:67:E5:11:0D:56
11:19:30 interface,info ether2 link down
11:42:46 dhcp,info dhcp1 deassigned 192.168.1.2 from D0:67:E5:11:0D:
15:58:38 dhcp,info dhcp1 assigned 192.168.1.2 to D0:67:E5:11:0D:56
15:58:38 interface,info ether2 link up (speed 100M, full duplex)
16:39:01 system,error,critical login failure for user admin from D0:
16:39:09 system,info,account user admin logged in from D0:67:E5:11:0
16:39:09 system,info,account user admin logged in via local
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah menu **Log**, seperti terlihat pada gambar berikut ini.



Gambar 10.3
Log

Dari gambar 10.3, terlihat bahwa terdapat beberapa aktifitas login, baik melalui WinBox maupun telnet. Juga terlihat adanya beberapa status *up* dan *down* dari interface *ether1* dan *ether2*. Juga terlihat bahwa terdapat user yang melakukan peminjaman IP Address dan tentunya banyak informasi lainnya.

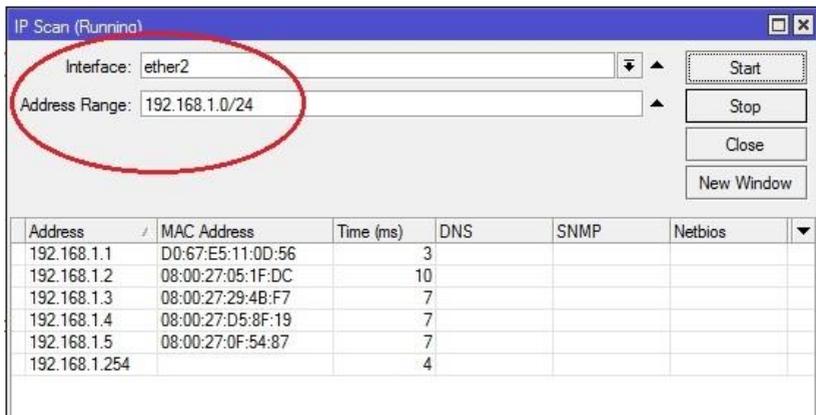
Monitoring User

Untuk monitoring user secara sederhana dapat dilakukan dengan melihat jumlah user yang terhubung ke jaringan Anda. Untuk melakukan monitoring jumlah user, dapat dilakukan dengan melihat berapa IP Address yang ada pada suatu jaringan. Dengan monitoring ini, juga akan bisa didapatkan informasi MAC Address dari setiap user.

Untuk mengetahui jumlah user berdasarkan IP Address yang mereka gunakan, Anda dapat memanfaatkan fitur IP Scan. Sebagai contoh, untuk melihat sejumlah IP Address pada range 192.168.1.0/24 yang terhubung pada interface *ether2*, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > tool ip-scan interface=ether2 \
address-range=192.168.1.0/24
Flags: D - dhcp
ADDRESS          MAC-ADDRESS      TIME  DNS   SNMP
192.168.1.1      D0:67:E5:11:0D:56 4ms
192.168.1.5      08:00:27:0F:54:87 6ms
192.168.1.4      08:00:27:D5:8F:19 6ms
192.168.1.3      08:00:27:29:4B:F7 6ms
192.168.1.2      08:00:27:05:1F:DC 5ms
192.168.1.254    6ms
-- [Q quit|D dump|C-z pause]
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Tools** → **IP Scan**, seperti terlihat pada gambar berikut ini.



Gambar 10.4
IP Scan

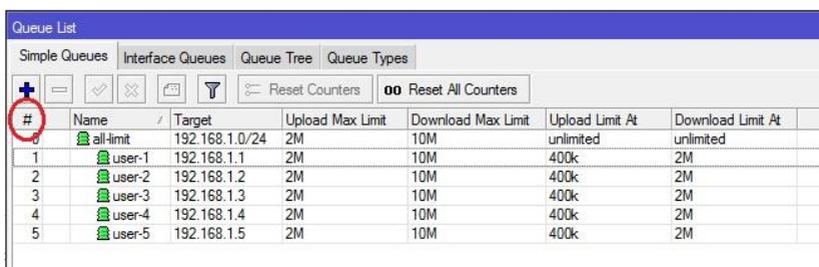
Dari gambar 10.4, terlihat bahwa pada jaringan 192.168.1.0/24 terdapat 5 (lima) user. Yang perlu diingat bahwa IP Scan bekerja berdasarkan range IP Address, sehingga jika pada suatu jaringan

terdapat user yang menggunakan IP Address yang tidak sesuai, maka bisa saja user tersebut tidak akan terlihat pada saat proses IP Scan.

Monitoring Bandwidth (Graph)

Yang tidak kalah penting dari keseluruhan proses monitoring adalah memantau penggunaan bandwidth. Pemantauan bandwidth dapat dilakukan terhadap alokasi bandwidth yang didapat dari ISP, bandwidth yang keluar masuk dari setiap interface, maupun alokasi bandwidth yang digunakan oleh setiap user.

Khusus untuk memantau penggunaan bandwidth dari setiap user, Anda harus mengaktifkan manajemen bandwidth dengan menggunakan Simple Queue. Ini karena monitoring bandwidth dari setiap user dapat dilihat dari traffic yang ditangani oleh setiap konfigurasi pada Simple Queue. Asumsi yang digunakan pada pembahasan ini adalah Router MikroTik yang memiliki jaringan 192.168.1.0/24 pada interface *ether2*. Dan pada jaringan tersebut sudah dikonfigurasi Simple Queue untuk menangani 5 (lima) user.



#	Name	Target	Upload Max Limit	Download Max Limit	Upload Limit At	Download Limit At
0	all-limit	192.168.1.0/24	2M	10M	unlimited	unlimited
1	user-1	192.168.1.1	2M	10M	400k	2M
2	user-2	192.168.1.2	2M	10M	400k	2M
3	user-3	192.168.1.3	2M	10M	400k	2M
4	user-4	192.168.1.4	2M	10M	400k	2M
5	user-5	192.168.1.5	2M	10M	400k	2M

Gambar 10.5
Konfigurasi Simple Queue

Mengaktifkan Graph

Router MikroTik menyediakan monitoring penggunaan bandwidth dalam bentuk grafik. Informasi dalam bentuk grafik ini bisa diakses dengan menggunakan web browser. Dengan demikian, sebelum melakukan monitoring, harus dipastikan bahwa service web atau HTTP pada Router MikroTik berada dalam posisi enable. Untuk memastikan service web (www) berjalan, dapat digunakan perintah pada bab sebelumnya, seperti pada uraian berikut ini.

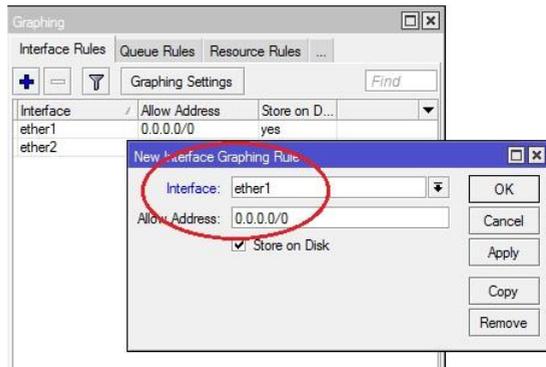
```
[admin@GATEWAY] > ip service print
Flags: X - disabled, I - invalid
#  NAME          PORT ADDRESS  CERTIFICATE
0  XI telnet      23
1  XI ftp         21
2  www           80
3  XI ssh        22
4  XI www-ssl    443         none
5  api           8728
6  winbox        8291
7  api-ssl       8729         none
```

Langkah berikutnya adalah mengaktifkan grafik untuk monitoring semua interface. Perintah yang dapat dilakukan adalah sebagai berikut.

```
[admin@GATEWAY] > tool graphing interface add interface=ether1
[admin@GATEWAY] > tool graphing interface add interface=ether2
[admin@GATEWAY] > tool graphing interface print
Flags: X - disabled
#  INTERFACE      ALLOW-ADDRESS  STORE-ON-DISK
0  ether1         0.0.0.0/0     yes
1  ether2         0.0.0.0/0     yes
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Tools** → **Graphing** → tab **Interface Rules**, tombol **Add**, seperti pada gambar berikut ini.

Gambar 10.6
Mengaktifkan grafik
untuk interface *ether1* dan
ether2



Dari uraian tadi dan gambar 10.6, Anda dapat menggunakan parameter *allow-address* untuk menentukan dari alamat IP Address mana saja informasi grafik ini bisa diakses. Jika suatu saat diinginkan informasi grafik ini hanya bisa diakses dari jaringan 192.168.1.0/24, maka perintah yang harus digunakan akan terlihat seperti uraian berikut.

```
[admin@GATEWAY] > tool graphing interface add
interface=ether1 allow-address=192.168.1.0/24 \

[admin@GATEWAY] > tool graphing interface add
interface=ether2 allow-address=192.168.1.0/24 \

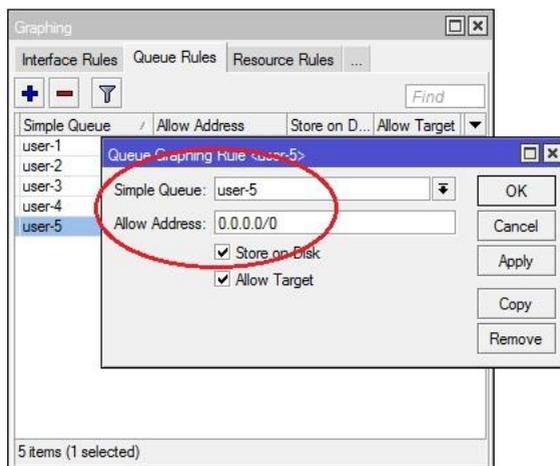
[admin@GATEWAY] > tool graphing interface print
Flags: X - disabled
#  INTERFACE          ALLOW-ADDRESS      STORE-ON-DISK
0  ether1              192.168.1.0/24    yes
1  ether2              192.168.1.0/24    yes
```

Jika ingin melakukan monitoring penggunaan bandwidth untuk setiap user, maka grafik dapat diaktifkan terhadap Simple Queue. Sebagai catatan, Anda tidak akan bisa melakukan monitoring alokasi bandwidth untuk setiap user, jika ternyata tidak ada konfigurasi Simple Queue untuk user tersebut.

Jika konfigurasi Simple Queue sudah dilakukan, untuk mengaktifkan grafik terhadap Simple Queue, maka perintah berikut ini dapat digunakan.

```
[admin@GATEWAY] > tool graphing queue add simple-queue=user-1  
[admin@GATEWAY] > tool graphing queue add simple-queue=user-2  
[admin@GATEWAY] > tool graphing queue add simple-queue=user-3  
[admin@GATEWAY] > tool graphing queue add simple-queue=user-4  
[admin@GATEWAY] > tool graphing queue add simple-queue=user-5
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Tools → Graphing → tab Queue Rules**, tombol **Add**, seperti pada gambar berikut ini.



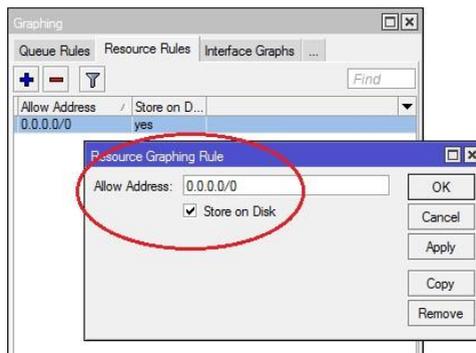
Gambar 10.7
Mengaktifkan grafik untuk Simple Queue

Selain itu, penggunaan resource router, seperti CPU, memori maupun disk juga dapat dimonitoring dalam bentuk grafik. Adapun perintah yang dapat digunakan adalah sebagai berikut.

```
[admin@GATEWAY] > tool graphing resource add  
allow-address=0.0.0.0/0 disabled=no
```

```
[admin@GATEWAY] > tool graphing resource print  
Flags: X - disabled  
# ALLOW-ADDRESS STORE-ON-DISK  
0 0.0.0.0/0 yes
```

Dengan menggunakan WinBox, menu yang dapat digunakan adalah **Tools → Graphing → tab Resource Rules**, tombol **Add**, seperti pada gambar berikut ini.

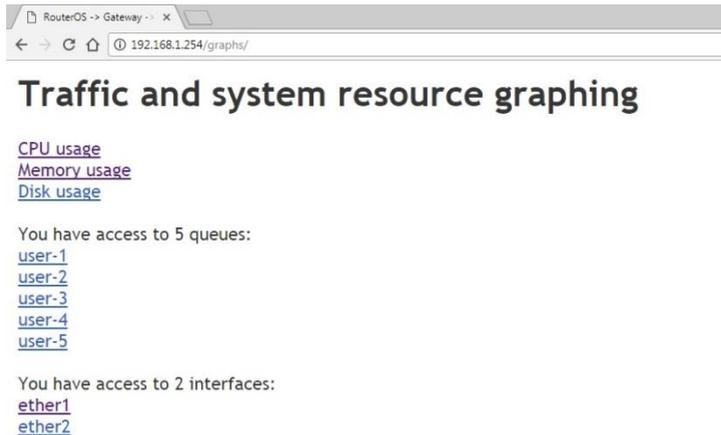


Gambar 10.8
Mengaktifkan grafik untuk resource router

Membaca Graph

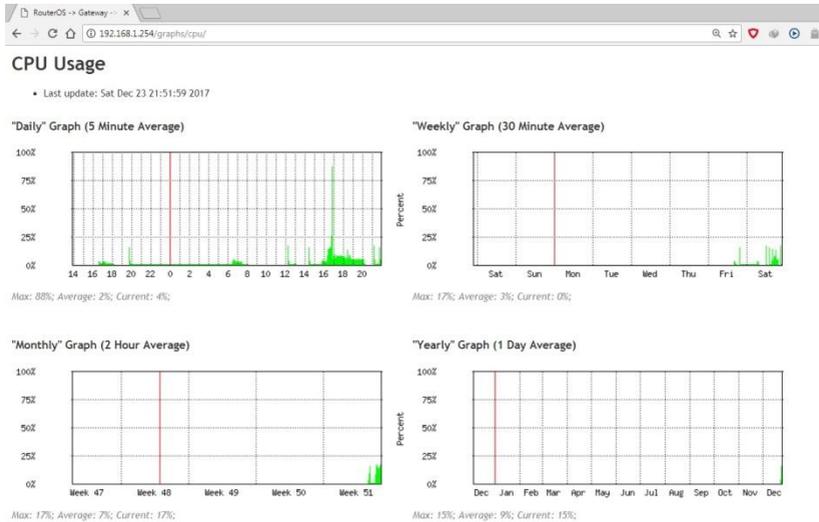
Pembacaan grafik penggunaan bandwidth, resource maupun Simple Queue dapat dilakukan dengan menggunakan web browser. Adapun format alamat yang dapat digunakan adalah **http://ipaddressrouter/graph**. Jika menggunakan skenario dengan IP

Address 192.168.1.254 pada interface *ether2*, maka alamat yang dapat digunakan adalah *http://192.168.1.254/graphs*, seperti pada gambar berikut ini.



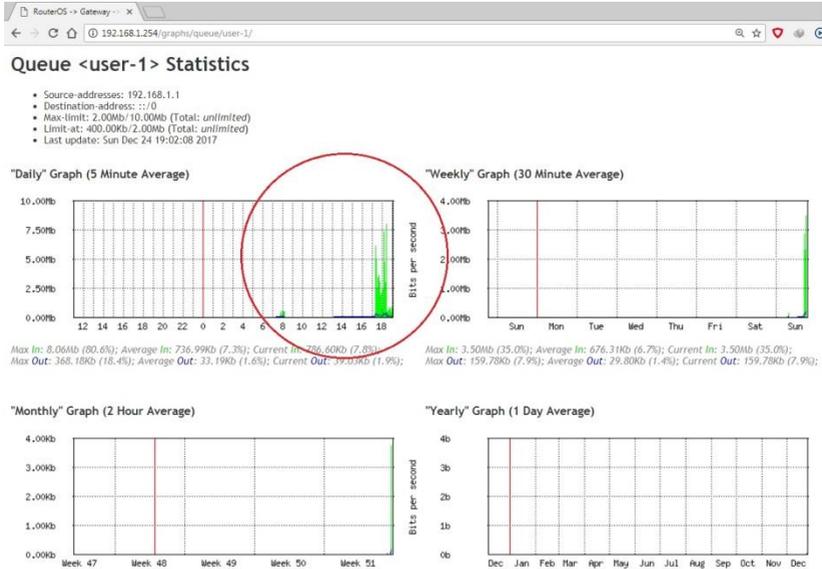
Gambar 10.9
Tampilah grafik monitoring

Untuk melihat pemakaian resource, link yang dapat digunakan adalah CPU usage, Memory usage dan Disk usage, seperti contoh gambar berikut ini.



Gambar 10.10
Grafik Pemakaian CPU

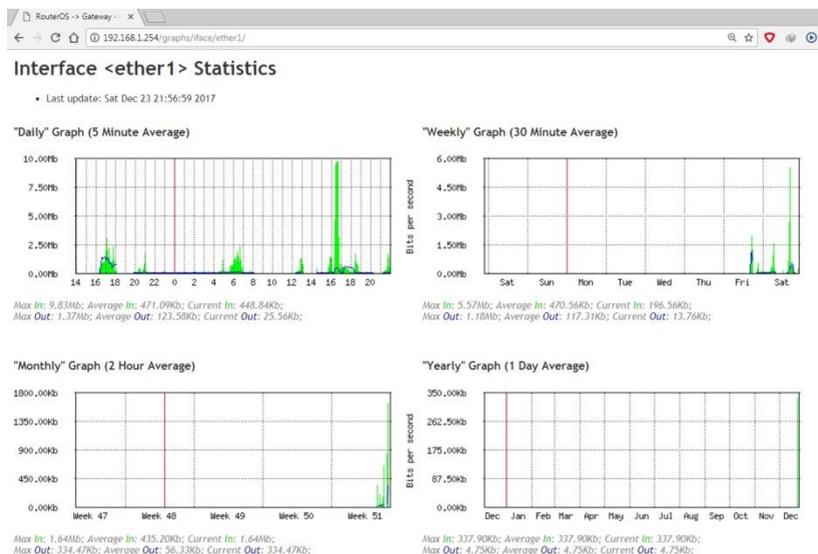
Sedangkan pemakaian bandwidth dari setiap user dapat diakses melalui link queue. Dalam contoh ini, jika ingin melihat pemakaian bandwidth *user-1*, maka link yang dapat digunakan adalah *user-1*, seperti terlihat pada gambar berikut ini.



Gambar 10.11
Grafik pemakaian bandwidth untuk *user-1*

Dari gambar 10.11, dapat dilihat pemakaian bandwidth dari *user-1*, baik itu alokasi upload maupun download. Untuk alokasi download dapat dibaca pada trafik **In** (berwarna hijau), sedangkan untuk trafik upload dapat dibaca pada trafik **Out** (garis biru).

Pada bagian grafik interface, terdapat pilihan beberapa link untuk setiap interface yang ada di Router MikroTik. Jika ingin melihat total bandwidth yang didapatkan (digunakan) dari ISP, maka Anda bisa menggunakan link interface *ether1*, seperti terlihat pada gambar berikut ini.



Gambar 10.12
 Grafik bandwidth pada *ether1*

Dari gambar 10.12, terlihat pemakaian bandwidth dari keseluruhan jaringan lokal. Untuk pemakaian bandwidth download dapat dilihat pada grafik **In** (warna hijau), sedangkan untuk pemakaian bandwidth upload dapat dilihat pada garfik **Out** (garis biru).

End of Chapter