

Published by Netlab | 2017

MODUL PRAKTIKUM

MANAJEMEN JARINGAN
KOMPUTER

NETLAB

MikroTik



Praktikum Management Jaringan

BAB I MANAGEMENT JARINGAN

1.1 Pengertian Management Jaringan

Definisi manajemen jaringan merupakan fungsi pengawasan terhadap sebuah jaringan komputer yang sedang berjalan, yang diharapkan adalah supaya jaringan selalu berjalan dengan baik dengan cara mengendalikan aliran trafik agar diperoleh kapasitas jaringan dengan pengoperasian maksimum dalam berbagai situasi.

Upaya mengkoordinasikan dan mendistribusikan sumberdaya (resource) untuk merencanakan, menganalisa, mengevaluasi, mendesain, mengadministrasikan, dan mengembangkan jaringan telekomunikasi sehingga diperoleh kualitas pelayanan yang baik pada seluruh waktu dengan biaya yang proporsional dan kapasitas yang optimal, atau melakukan monitoring atau mengontrol sebuah jaringan secara berkala.

1.1.1 Fungsi Management Jaringan

1. Manajemen Kesalahan (FaultManagement), menyediakan fasilitas yang memungkinkan administrator jaringan untuk mengetahui kesalahan (fault) pada perangkat yang dikelola, jaringan, dan operasi jaringan, agar dapat segera menentukan apa penyebabnya dan dapat segera mengambil tindakan (perbaikan). Untuk itu, manajemen kesalahan memiliki mekanisme untuk :
 - Melaporkan terjadinya kesalahan
 - Mencatat laporan kesalahan (logging)
 - Melakukan diagnosis
 - Mengoreksi kesalahan (dimungkinkan secara otomatis)
2. Manajemen Konfigurasi (Configuration Management), memonitor informasi konfigurasi jaringan sehingga dampak dari perangkat keras atau pun lunak tertentu dapat dikelola dengan baik. Hal tersebut dapat dilakukan dengan kemampuan untuk inisialisasi, konfigurasi ulang, pengoperasian, dan mematikan perangkat yang dikelola.



Praktikum Management Jaringan

3. Pelaporan (Accounting), mengukur utilisasi jaringan dari pengguna atau grup tertentu untuk:
 - Menghasilkan informasi tagihan (billing)
 - Mengatur pengguna atau grup
 - Membantu dalam menjaga performa jaringan pada level tertentu yang dapat diterima
 - Manajemen Performa (Performance Management), mengukur berbagai aspek dari performa jaringan termasuk pengumpulan dan analisis dari data statistik sistem sehingga dapat dikelola dan dipertahankan pada level tertentu yang dapat diterima. Untuk itu, manajemen performa memiliki kemampuan untuk:
 - Memperoleh utilisasi dan tingkat kesalahan dari perangkat jaringan
 - Mempertahankan performa pada level tertentu dengan memastikan perangkat memiliki kapasitas yang mencukupi.
4. Manajemen Keamanan (SecurityManagement), mengatur akses ke sumber daya jaringan sehingga informasi tidak dapat diperoleh tanpa izin. Hal tersebut dilakukan dengan cara :
 - Membatasi akses ke sumber daya jaringan
 - Memberi pemberitahuan akan adanya usaha pelanggaran dan pelanggaran keamanan

1.1.2 Prinsip Prinsip Dasar Pemeliharaan Jaringan

Untuk dapat menerapkan strategi umum diatas, bisa digunakan beberapa prinsip dasar Pemeliharaan Jaringan sebagai berikut :

1. Preventive Maintenance

Pemeliharaan jaringan yang dilaksanakan secara berkala, atau menurut kriteria yang telah ditetapkan, dengan tujuan mengurangi kemungkinan gangguan dan mencegah elemen dari degradasi fungsi.



Praktikum Management Jaringan

2. Corrective Maintenance

Pemeliharaan yang dilaksanakan setelah diketahui adanya gangguan dengan tujuan untuk memperbaiki sehingga dapat berfungsi seperti sediakala .

3. Controlled Maintenance

Filosofi dasar diatas bisa diterapkan pada network elemen analog, campuran analog –digital mapun digital penuh. Akan tetapi Controlled Maintenance akan lebih cocok diterapkan pada Network Digital, untuk perangkat Analog dibutuhkan tambahan External Maintenance Tool.

Adapun contoh kasus manajemen jaringan yang sering terjadi di lingkungan masyarakat disuatu perusahaan besar yang memiliki banyak gedung perkantoran, manajemen jaringan sangat diperlukan. Dimana ada satu titik pusat yang mengendalikan dan mengawasi arus data yang masuk maupun yang keluar.

1.2 Cara Membuat Sebuah Konsep Jaringan

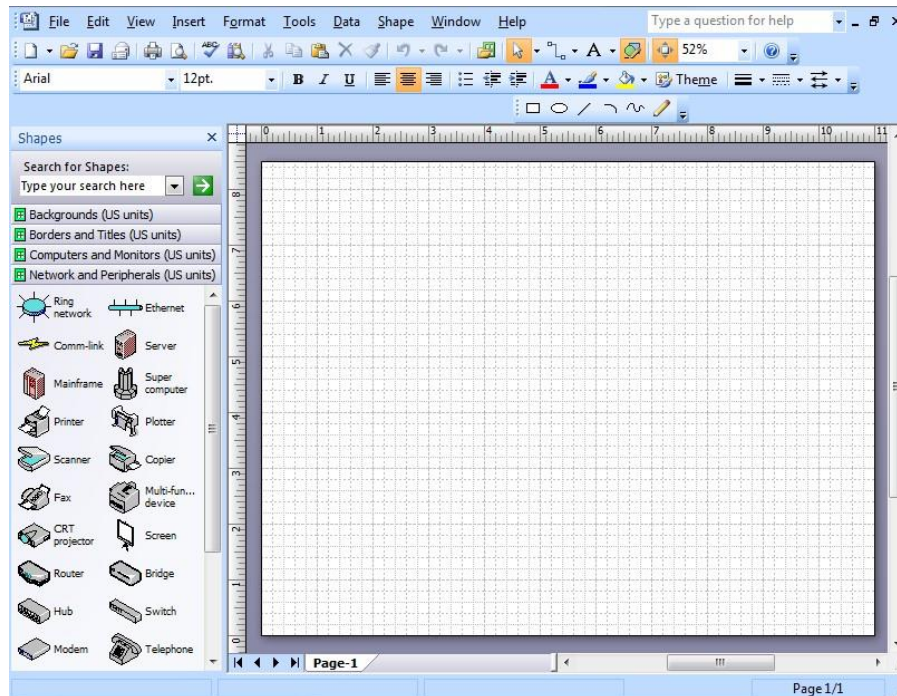
Dalam pembuatan desain jaringan pada windows kita dapat menggunakan aplikasi “Visio” sebagai medianya. Pada proses pembuatan desain jaringan sebelumnya yang kita dapat pada pelajaran Jaringan Komputer yang di mana kita menggunakan cisco packet tracer sebagai medianya sekaligus desainnya sekarang akan kita pisahkan antara desain dan pengerjaanya pada desain kita menggunakan media Visio dan pada pengerjaanya langsung menggunakan mikrotik.



Praktikum Management Jaringan

1.3 Penjelasan Tools Pada Microsoft Visio 2007

Pada Microsoft visio terdapat tool yang digunakan pada proses pengerjaanya dimana pada windows yang di desain untuk pembuatan simulasi berbasis grafis maka fitur yang di berikan cukup lengkap dan kompleks, adapun tampilan fitur yang terdapat pada Visio adalah sebagai berikut.

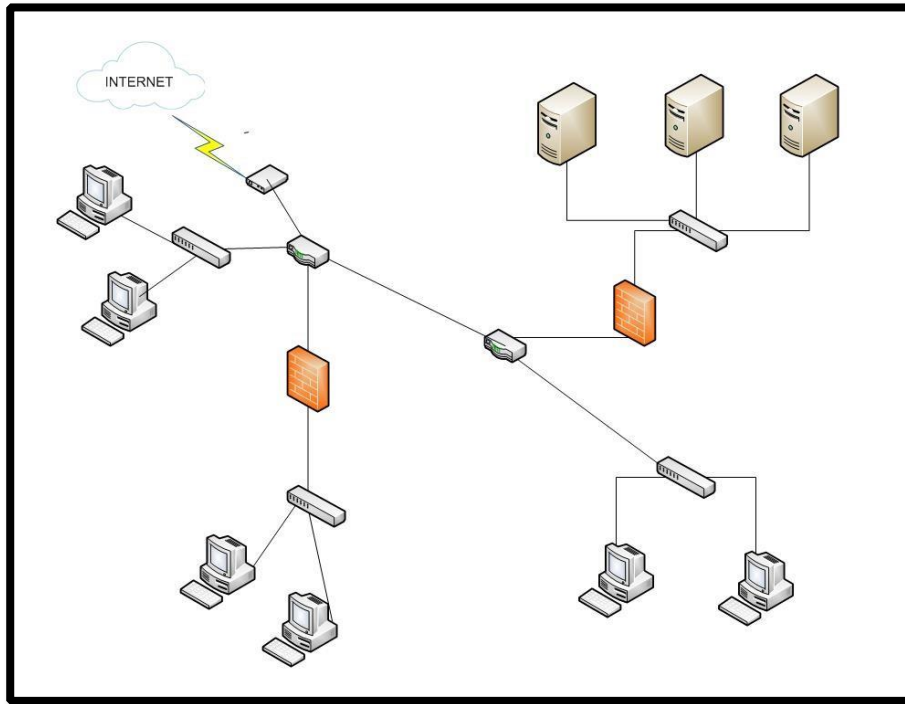


Gambar 1.2 tampilan *fiture-fiture* yang di sediakan oleh office visio

Tools yang di sediakan Visio memungkinkan dalam pembuatan desain yang kompleks termasuk jenis- jenis keamanan apa yang ingin kita terapkan pada desain jaringan yang telah kita buat, Visio memungkinkan kita untuk membuat sebuah desain yang mudah di mengerti oleh konsumen dengan konsep yang kita terapkan di kehidupan nyata. Adapun konsep minimalis yang dapat dibuat kurang lebih seperti pada gambar berikut ini:



Praktikum Management Jaringan



Gambar 1.3 contoh design jaringan pada office visio

1.4 Routing

Pengaturan Routing Static

Routing merupakan teknik yang digunakan untuk menghubungkan beberapa jaringan yang memiliki network address maupun teknologi yang berbeda beda dalam memanajemen sebuah jaringan. Routing merupakan materi pokok yang harus di kuasai oleh praktikan dalam praktikum ini, routing juga dapat memberikan jalur terbaik yang di tempuh paket data dalam melakukan pengiriman data “best path”.

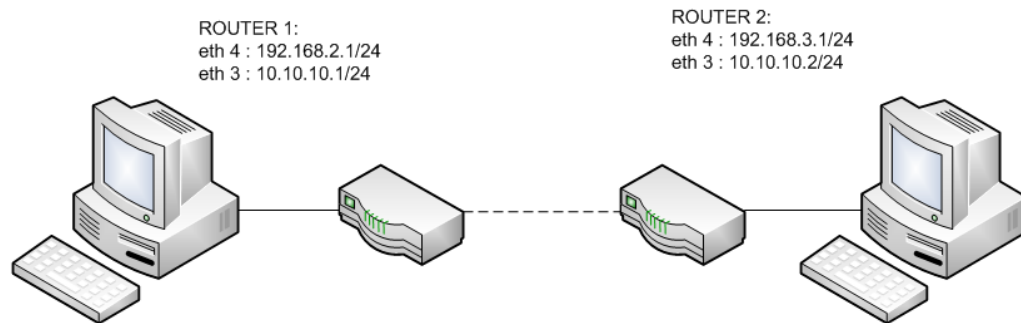
Konsep static routing

Sebelum menerapkan routing static secara nyata sebaiknya kita sedikit mengulas pemahaman dari routing static itu sendiri , karena bila anda terjun ke lapangan tentu anda akan dihadapkan dengan topologi jaringan yang berbeda beda topologi yang intinya akan sama dan tidak jauh berbeda seperti pengaturan routing di lapangan ,untuk mempermudah



Praktikum Management Jaringan

konsep routing static disini menerapkan sebuah topologi sederhana seperti pada gambar 1.4



Gambar 1.4 jaringan sederhana dengan 2 buah router

Sebagai langkah awalan konfigurasi ip address pada setiap interface yang ada pada router 1 dan router 2 yang sudah di jelaskan pada semester sebelumnya, kami tidak lagi menjelaskan secara panjang lebar dalam praktikum kali ini, bila mengalami kesulitan dalam pengisian ip router anda dapat membuka kembali modul jarkom pada semester ganjil, bila IP address telah terisi dengan benar seharusnya akan muncul tampilan seperti pada gambar 1.5 dan untuk router dua pada gambar 1.6.

Untuk melakukan routing tentunya kita harus konfigurasi IP pada mikrotik. Untuk Router 1 pada ether 4 diberikan IP 192.168.2.1 selanjutnya pada ether 1 di berikan IP 10.10.10.1 untuk konfigurasi IP seperti di bawah ini

Konfigurasi pada router 1

1. Konfigurasi IP pada ether 4

```
[admin@MikroTik] > ip address add address=192.168.2.1/24 interface=ether4
```

Gambar 1.5 Tampilan konfigurasi pada ether 4

2. Konfigurasi IP pada ether 3

```
[admin@MikroTik] > ip address add address=10.10.10.1/24 interface=ether3
```

Gambar 1.6 Tampilan konfigurasi pada ether 3



Praktikum Management Jaringan

Konfigurasi pada router 2

1. Konfigurasi IP pada ether 4

```
[admin@MikroTik] > ip address add address=192.168.3.1/24 interface=ether4
```

Gambar 1.7 Tampilan konfigurasi pada ether 4

2. Konfigurasi IP pada ether 3

```
[admin@MikroTik] > ip address add address=10.10.10.2/24 interface=ether3
```

Gambar 1.8 Tampilan konfigurasi pada ether 3

Untuk melakukan teknik routing anda harus dapat membaca table routing itu sendiri, tabel pada router yang digunakan sebagai pedoman untuk menuju suatu jaringan atau network, table ini dapat dikatakan sebagai peta pada router tersebut. Router tidak dapat menjangkau suatu jaringan jika network address dari jaringan tidak ada dalam table routing, tentunya anda akan kesulitan bila mencari data yang tidak ada di dalam peta. Untuk melihat peta router pada router 1 dan router 2 anda dapat mengetikkan perintah berikut seperti pada gambar 1.9 dan untuk router 2 seperti pada gambar 1.10.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK    INTERFACE
0  192.168.2.1/24     192.168.2.0 ether4
1  10.10.10.1/24      10.10.10.0 ether3
```

Gambar 1.9 Tampilan ip pada router 1

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK    INTERFACE
0  192.168.3.1/24     192.168.3.0 ether4
1  10.10.10.2/24      10.10.10.0 ether3
```

Gambar 1.10 Tampilan ip pada router 2



Praktikum Management Jaringan

Jika anda memperhatikan dengan seksama table routing tersebut, table routing pada router 1 tidak berisi informasi tentang network 192.168.3.0 begitu juga dengan router 2 dimana tidak berisi informasi tentang Ethernet dengan ip 192.168.2.0 dengan kata lain router masih belum dapat terhubung. Pada kondisi ini table routing pada router masih belum lengkap, untuk melengkapinya anda harus melakukan routing static ataupun dynamic.

Sebelum terlalu jauh anda harus memahami konsep dari routing itu sendiri, anda ingin lewat jalur mana dan mau kemana. Sebagai langkah pertama marilah kita jadikan router 1 sebagai acuan terlebih dahulu bila kita ingin menuju dari IP 192.168.2.0 dan ingin ke ip 192.168.3.0 kita harus melewati router 1 dengan ip 10.10.10.1 dan melalui router 2 dengan alamat IP 10.10.10.2 nah di setiap langkah ini di perlukan yang namanya gateway atau mudah di ibaratkan sebagai pintu masuk, dikarenakan bila ip berbeda hanya router yang dapat menyatukannya atau menghubungkannya. Adapun langkah yang selanjutnya akan di lakukan adalah sebagai berikut :

```
[admin@R1]> ip route add dst-address=192.168.3.0/24  
gateway=10.10.10.2
```

```
[admin@MikroTik] > ip route add dst-address=192.168.3.0/24 gateway=10.10.10.2
```

Gambar 1.11 Tampilan routing pada router 1

Dan untuk router 2 memiliki script sendiri sebagai berikut :

```
[admin@R1]> ip route add dst-address=192.168.2.0/24 gateway=10.10.10.1
```

```
[admin@MikroTik] > ip route add dst-address=192.168.2.0/24 gateway=10.10.10.1
```

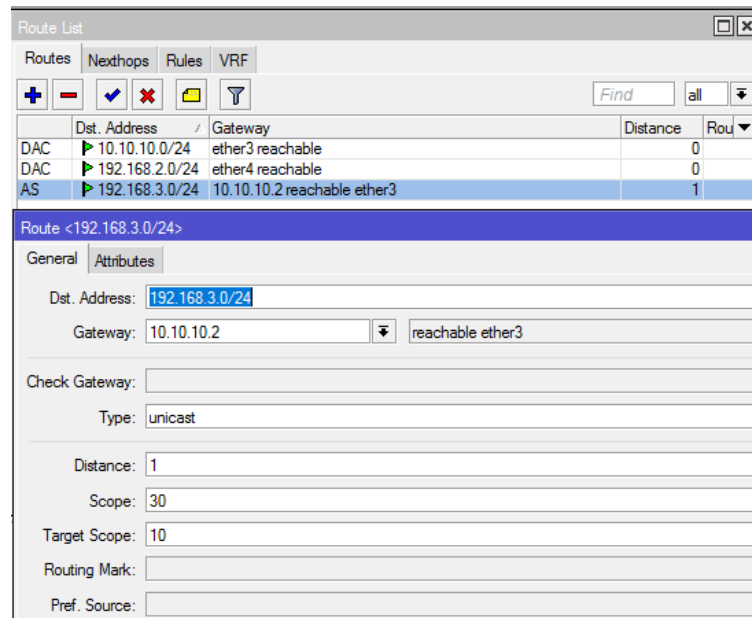
Gambar 1.12 Tampilan routing pada router 2



Praktikum Management Jaringan

Jika anda ingin melakukan pengaturan menggunakan gui anda dapat melakukannya dengan cara mengklik winbox kalian pada menu IP – Routes dan klik pada ip yang ingin di masukan alamatnya.

Adapun tampilanya seperti pda gambar 1.13 sebagai berikut:



Gambar 1.13 pengisian dst address

Setelah konfigurasi routing static selesai langkah selanjutnya adalah dengan mengetikkan script di tabel pada New terminal pada webfix kalian seperti pada gambar 1.14 :

```
[admin@r1]ip route print
```

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS      PREF-SRC  GATEWAY      DISTANCE
0   ADC 10.10.10.0/24  10.10.10.1  ether3        0
1   ADC 192.168.2.0/24  192.168.2.1 ether4        0
2   A S  192.168.3.0/24      10.10.10.2  1
```

Gambar 1.14 Tampilan route pada router 1



Praktikum Management Jaringan

```
[admin@r2]ip route print
```

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#       DST-ADDRESS      PREF-SRC  GATEWAY            DISTANCE
0 ADC   10.10.10.0/24      10.10.10.2 ether3             0
1 A S    192.168.2.0/24         10.10.10.1         1
2 ADC   192.168.3.0/24      192.168.3.1 ether4             0
```

Gambar 1.15 Tampilan route pada router 2

Untuk membuktikan bahwa PC 1 dan PC 2 kita akan membuktikan dengan perintah ping
Pengujian Ping dari PC 1 ke PC 2. Pada konfigurasi ip di PC 2 dengan alamat ip 192.168.3.2

```
C:\Users\Netlab>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Gambar 1.16 Pengujian koneksi dari PC 1 ke PC 2

Pengujian perintah ping dari PC 2 ke PC 1. Pada konfigurasi ip di PC 1 dengan alamat ip 192.168.2.2

```
C:\Users\Jenk>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.3.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Gambar 1.17 Pengujian koneksi dari PC 2 ke PC 1



Praktikum Management Jaringan

Gambar di atas merupakan gambar dari route print yang dimiliki oleh masing-masing mikrotik, setelah pengaturan routing mikrotik selesai periksalah kembali pada table routing anda apakah hasilnya sudah sama dengan yang ada pada gambar di atas. Anda dapat melihat table routing pada r1 lengkap karena telah berisi informasi network 192.168.3.0/24 dengan gateway 10.10.10.2 .begitu juga dengan network yang berisi IP 192.168.2.0 yang berisi gate way 10.10.10.1 bila langkah yang di lakukan sudah benar seharusnya PC1 dengan PC 2 sudah dapat terhubung .



BAB II FIREWALL

2.1. Pengantar Firewall

Firewall adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar. Firewall merupakan sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar. Firewall digunakan untuk memastikan bahwa data pada komputer atau server Web yang terhubung tidak akan bisa diakses siapa saja di Internet. Pihak lain yang mengakses informasi pribadi atau mengubah situs Web anda akan di blokir oleh Firewall.

Firewall dapat berarti suatu mekanisme/sistem/cara yang diterapkan baik terhadap suatu sistem pada jaringan, software, atau hardware itu sendiri dengan tujuan melindungi (membatasi, menyaring, dan menolak) suatu kegiatan pada jaringan yang sifatnya pribadi dengan jaringan luar yang tidak pada ruang lingkupnya. Firewall didesain agar dapat mengijinkan data yang dipercaya untuk lewat, mencegah jaringan internal dari luar yang sewaktu-waktu bisa masuk firewall, serta dapat menolak layanan yang sering diserang.



2.2. Firewall Network Address Translation (NAT)

Network Address Translation (NAT) adalah proses di mana perangkat jaringan, biasanya firewall, memberikan alamat publik ke komputer (atau kelompok komputer) dalam jaringan lokal. Penggunaan utama dari NAT untuk membatasi jumlah alamat IP publik suatu organisasi atau perusahaan menggunakan IP Publik, baik untuk tujuan ekonomi atau tujuan



Praktikum Management Jaringan

keamanan NAT adalah aspek yang sangat penting dari keamanan firewall. Untuk menghemat jumlah alamat publik yang digunakan dalam sebuah organisasi, dan memungkinkan untuk kontrol ketat dari akses ke sumber daya di kedua sisi firewall.

Selain itu, NAT dapat digunakan untuk memungkinkan akses selektif ke luar jaringan, juga. Workstation atau komputer lain yang membutuhkan akses khusus di luar jaringan dapat ditugaskan IP eksternal tertentu menggunakan NAT, yang memungkinkan mereka untuk berkomunikasi dengan komputer dan aplikasi yang memerlukan alamat IP publik yang unik.

Sekali lagi, firewall bertindak sebagai perantara, dan dapat mengontrol sesi di kedua arah, pelabuhan dan membatasi akses protokol.

Ada dua jenis NAT:

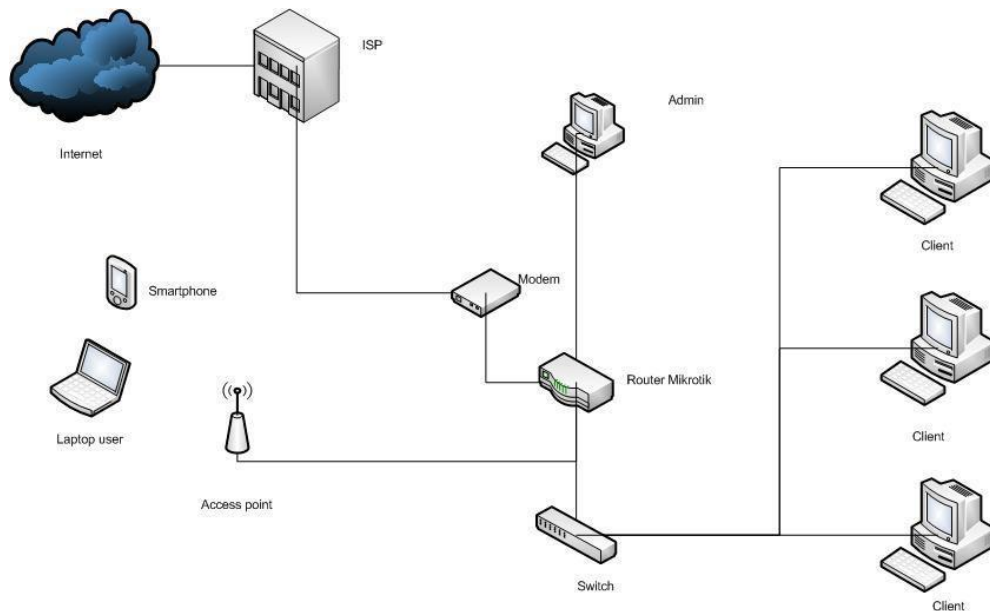
1. Chain Source NAT (srcnat) digunakan untuk merubahfiled IP address pengirim maupun port pengirim yang ada pada paket
2. Destination NAT(dsnat), digunakan untuk merubah IP address tujuan maupun tujuan yang ada pada paket

2.2.1. Konfigurasi NAT

1. Pengaturan NAT di lakukan agar setiap client atau user mendapat ip dari ISP, Yang pertama buatlah simulasi jaringan seperti pada gambar 2.1 dimana maksud dari simulasi ini adalah bagaimana kita dapat menghubungkan mikrotik dengan internet dengan bantuan pc user yang nantinya pengguna lain dapat terhubung dengan internet ketika terhubung ke mikrotik.



Praktikum Management Jaringan



Gambar 2.1 tampilan simulasi

2. Lalu bukalah aplikasi winbox seperti pada gambar 2.2 berikut ini:

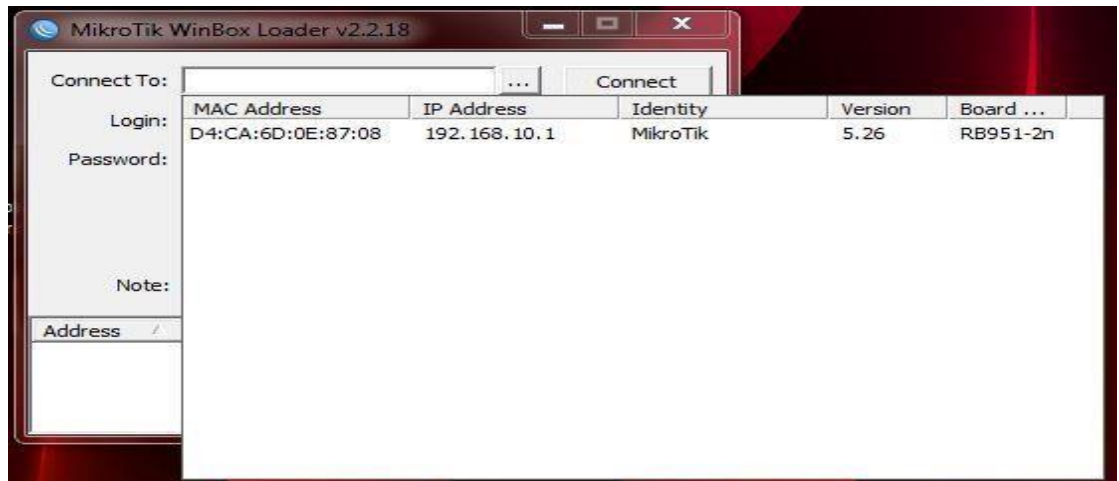


Gambar 2.2 gambar tampilan winbox

3. Langkah ketiga lakukan pengecekan apakah mikrotik anda telah ter deteksi oleh winbox atau belum dengan cara meng clic *button* (...) maka akan tampil gambar seperti pada Gambar 2.3 berikut ini.



Praktikum Management Jaringan



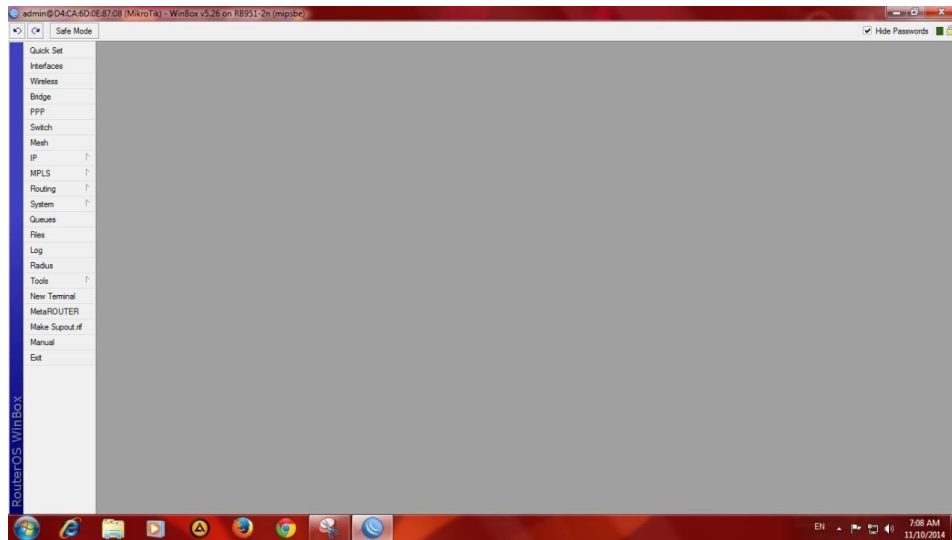
Gambar 2.3 tampilan pencarian Mikrotik

4. Bila device telah di temukan oleh winbox lalu saat inilah kita mulai masuk ke langkah seting mikrotik . jumlah MAC address tergantung jumlah mikrotik yang terhubung dengan pc client pada pengaturan ini terdapat 3 jenis pengaturan dengan media yang berbeda :
- a) menggunakan kabel LAN,
 - b) menggunakan WIFI dengan bantuan webfig,
 - c) menggunakan telnet dengan bantuan CLI

langkah yang di lakukan berikutnya dalah memasuki router os dengan cara menekan tombol connect pada tampilan winbox, seperti pada gambar 2.4.

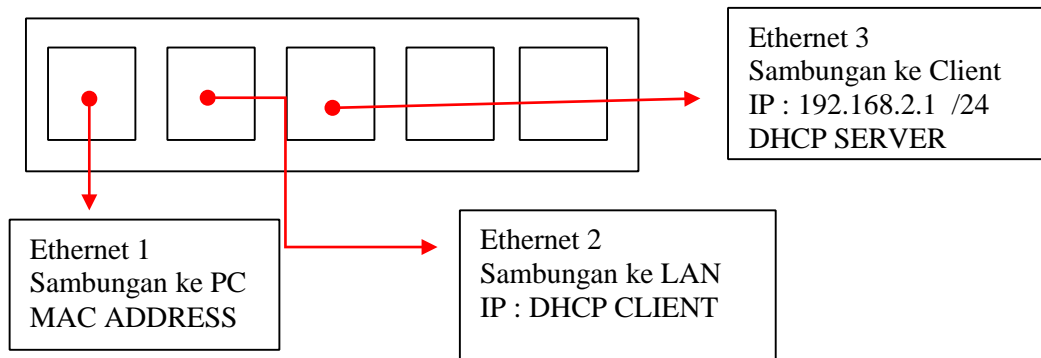


Praktikum Management Jaringan



Gambar 2.4 Tampilan Router OS

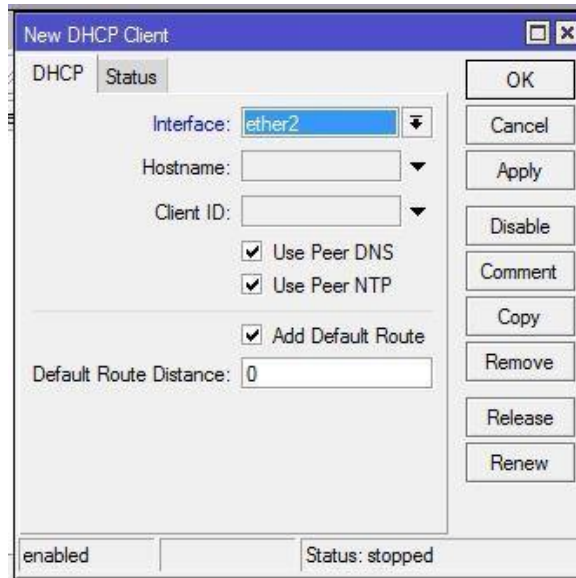
- Setelah dapat masuk pada aplikasi winbox pastikan IP Address pada Ethernet 1 sudah di setting seperti pada praktikum BAB 1 yaitu menggunakan MAC ADDRESS.
- Sebelum lebih jauh, harus dipahami bahwa pembagian port pada mikrotik adalah sebagai berikut :



- Setelah IP Address pada Ethernet 1 sudah sesuai maka lakukan konfigurasi IP pada Ethernet 2 yang merupakan DHCP Client dan Ethernet 3 yang merupakan DHCP Server.
- Untuk Ethernet 2 : Klik pada bagian **IP – DHCP CLIENT**. Setelah itu akan muncul window New DHCP Client seperti pada gambar 2.5. Kemudian set **interface** dengan **ether 2** klik **APPLY – OK**.

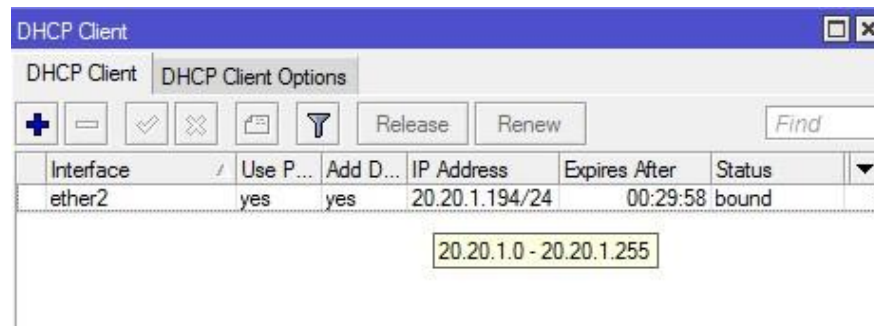


Praktikum Management Jaringan



Gambar 2.5 window New DHCP Client

9. Kemudian akan nampak hasil dari pengaturan DHCP Client yang telah kita atur tadi seperti pada gambar 2.6. IP address didapatkan secara DHCP dari server LAN dan status bound menunjukkan telah terkoneksi dengan baik.

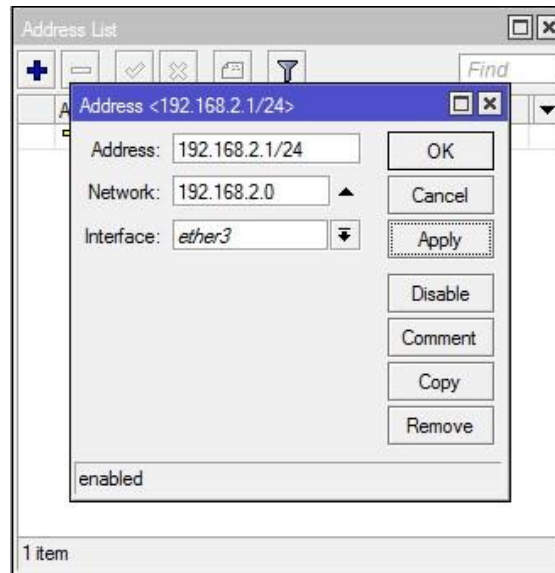


Gambar 2.6 Hasil Konfigurasi DHCP Client pada Ether 2

10. Setelah melakukan Konfigurasi IP Address pada Ether 2. Sekarang lakukan konfigurasi IP Address pada Ether 3 yaitu sebagai DHCP Server
11. Klik **IP – Address** kemudian tambahkan IP Address untuk Ether 5 yaitu 192.168.10.1 /24 seperti pada gambar 2.7

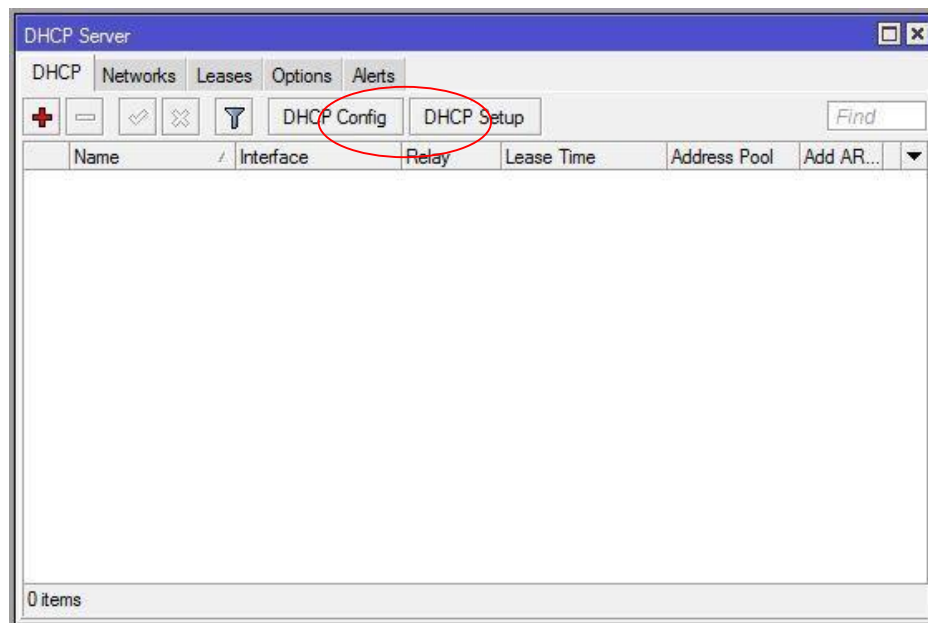


Praktikum Management Jaringan



Gambar 2.7 Konfigurasi IP address pada Ether 3

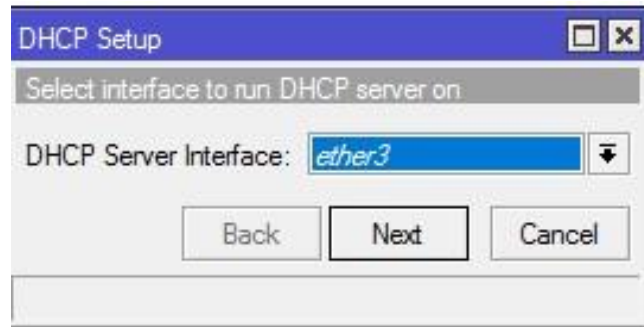
12. Klik **IP – DHCP SERVER** maka akan muncul window seperti pada gambar 2.8.
kemudian pilih tab **DHCP Setup**.



Gambar 2.8 DHCP Server Window

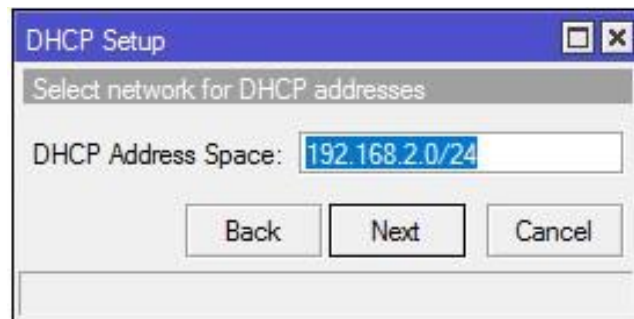


Praktikum Management Jaringan



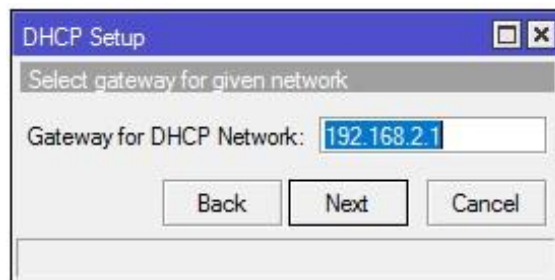
Gambar 2.9 Konfigurasi DHCP interface

13. Window DHCP Setup akan muncul, pastikan isi dari DHCP Address Space sudah seperti pada gambar 2.10 kemudian klik **Next**



Gambar 2.10 DHCP Setup Address Space

14. Selanjutnya isikan **Gateway for DHCP Network** yaitu 192.168.2.1 seperti pada gambar 2.11

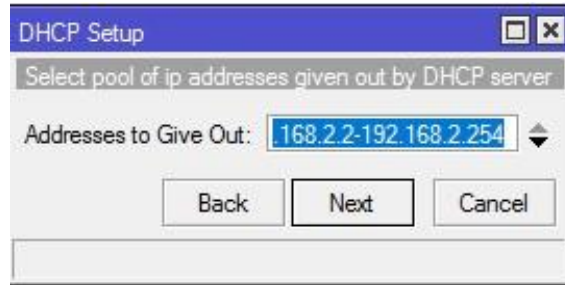


Gambar 2.11 Gateway for DHCP Network

15. Selanjutnya pada **Address to Give Out** merupakan range IP address yang akan di share pada client yaitu 192.168.2.2 – 192.168.2.254 seperti pada gambar 2.12.

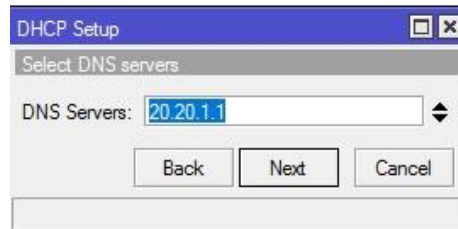


Praktikum Management Jaringan



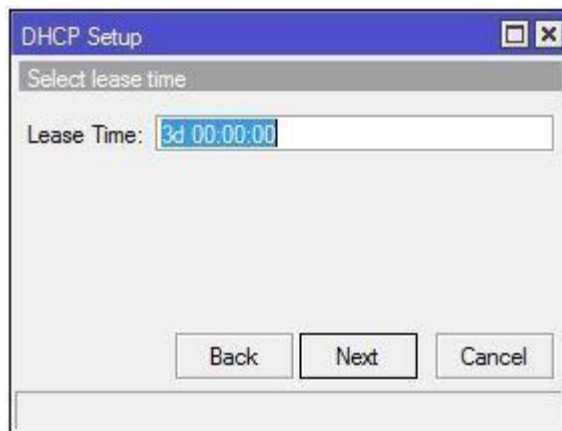
Gambar 2.12 Address to Give Out

16. Kemudian isikan **DNS Servers** seperti pada gambar 2.13 yaitu 20.20.1.1



Gambar 2.13 DNS Servers

17. Selanjutnya pada **Lease Time** langsung **Next** saja, biarkan seperti default yang ditunjukkan pada gambar 2.14.

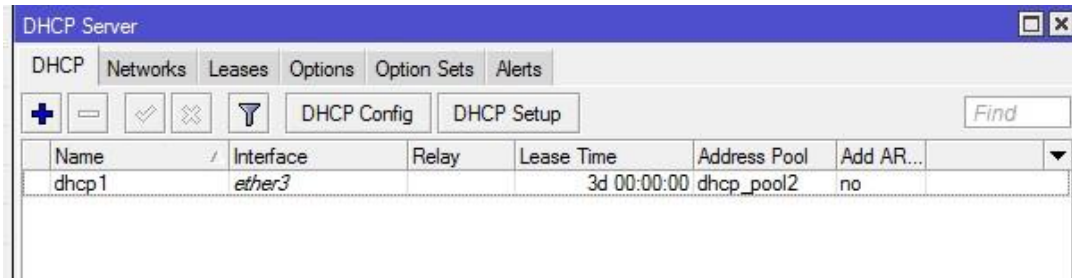


Gambar 2.14 Lease Time

18. Hasil dari konfigurasi DHCP Server untuk ether 5 akan tampak seperti pada gambar 2.15 dibawah ini :

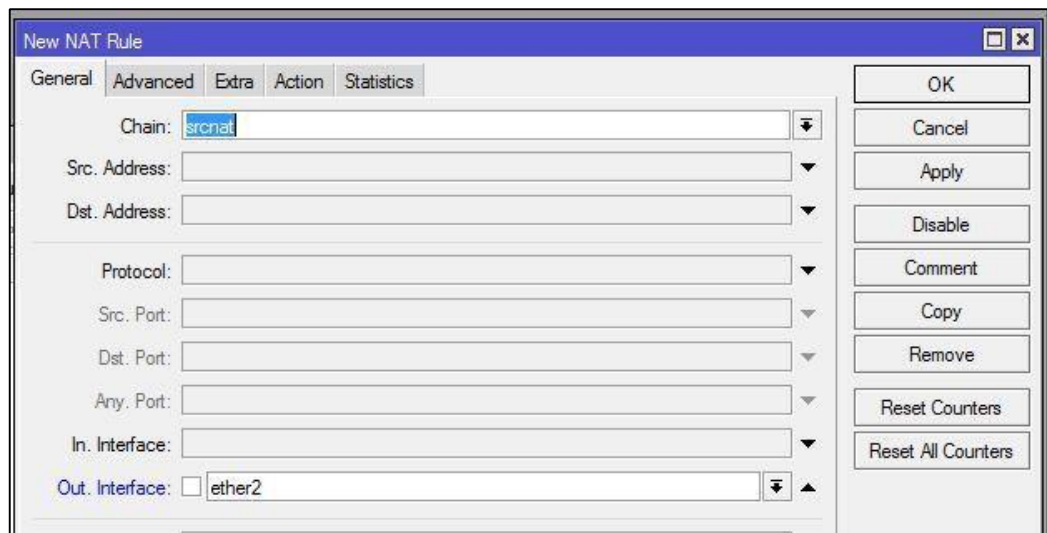


Praktikum Management Jaringan



Gambar 2.15 Hasil Konfigurasi DHCP Server untuk ether 3

19. Disinilah kita akan melakukan penambahan **NAT Rule**. Klik **IP – FIREWALL**.
Kemudian tambahkan rule nat baru.
20. Pada window **New NAT Rule** isikan **Chain : srcnat**, dan **Out. Interface : ether2** yang merupakan sumber internet pada mikrotik. Seperti pada gambar 2.16 dibawah ini :

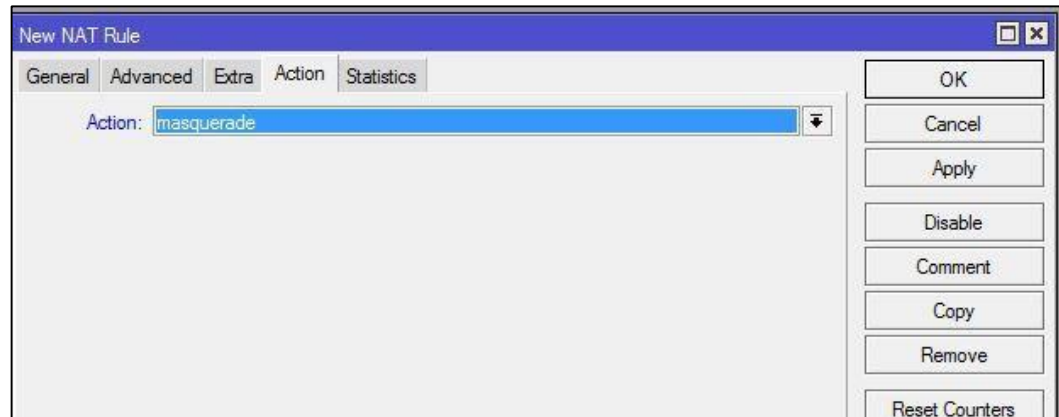


Gambar 2.16 New NAT Rule



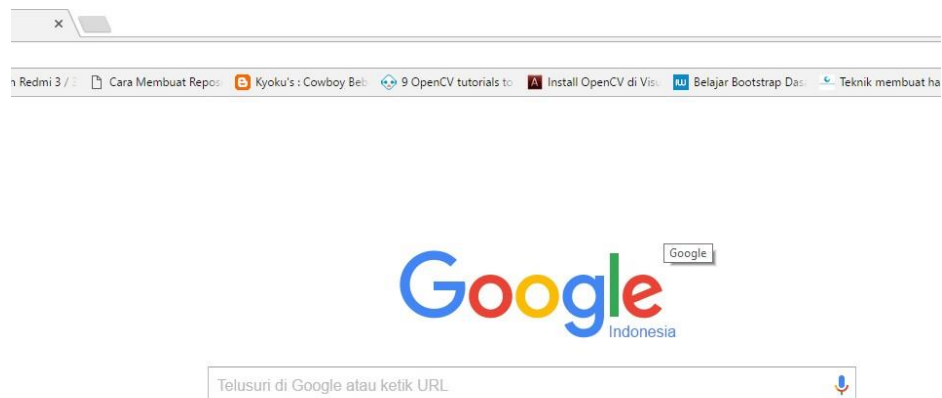
Praktikum Management Jaringan

21. Berpindah ke tab **Action** dan isikan **action** dengan **masquerade** seperti ditunjukkan pada gambar 2.17 kemudian klik **Apply – OK**



Gambar 2.17 Action Tab New NAT Rule

22. Setelah selesai lakukan uji coba keberhasilan NAT dengan membuka google pada browser seperti pada gambar 2.18



Gambar 2.18 Hasil Pengujian NAT

2.3.1 Web Proxy dengan Firewall (Layer7)

Protokol Layer7 adalah metode untuk mencari pola dalam ICMP / TCP / UDP stream, atau istilah lainnya regex pattern. Cara kerja L7 adalah mencocokkan (matcher) 10 paket koneksi pertama atau 2KB koneksi pertama dan mencari pola/pattern data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, matcher tidak memeriksa lebih lanjut. Dan akan dianggap unknown connections. Anda harus mempertimbangkan bahwa banyak



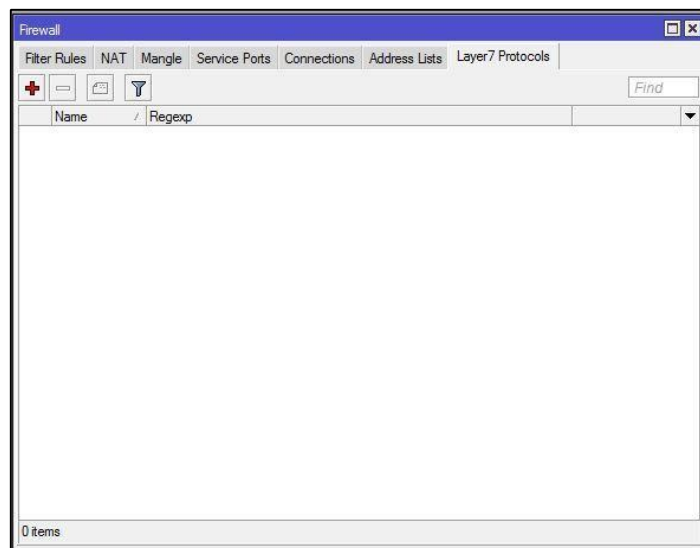
Praktikum Management Jaringan

koneksi secara signifikan akan meningkatkan penggunaan memori pada RB maupun PC Router anda. Untuk menghindari itu tambahkan regular firewall matchers (pattern) untuk mengurangi jumlah data yang dikirimkan ke layer-7 filter.

Layer7 matcher harus melihat kedua arah lalu lintas (masuk dan keluar). Untuk memenuhi persyaratan ini rule 17 harus diatur dalam chain Forward. Jika rule pada chain input/prerouting maka aturan yang sama harus diatur juga dalam chain output/postrouting, jika tidak maka data mungkin dianggap tidak lengkap sehingga pola/pattern dianggap tidak benar /cocok.

Konfigurasi Web Proxy dengan Firewall :

1. Masuk ke menu **IP – Firewall – tab Layer 7 Protocols** seperti pada gambar 2.23



Gambar 2.23 Firewall tab Layer 7 Protocols



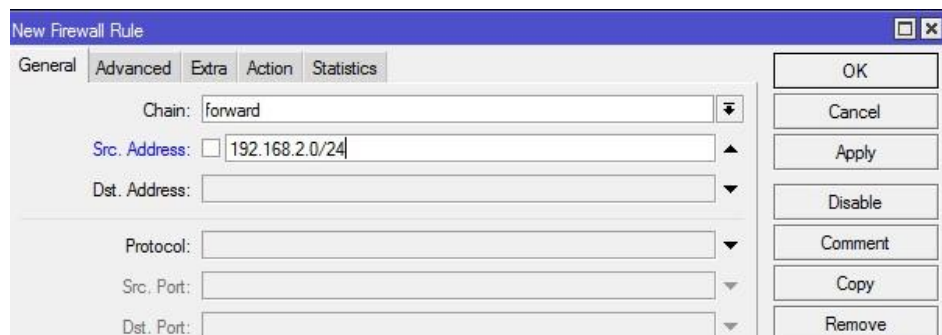
Praktikum Management Jaringan

2. Kemudian tambahkan **new firewall L7 protocols**, masukan alamat facebook yang akan di blok seperti pada gambar 2.24



Gambar 2.24 New Firewall L7 Protocols

3. Disinilah kita akan melakukan penambahan **NAT Rule**. Klik **IP – FIREWALL**. Kemudian tambahkan rule nat baru pada **tab general** seperti pada gambar 2.25

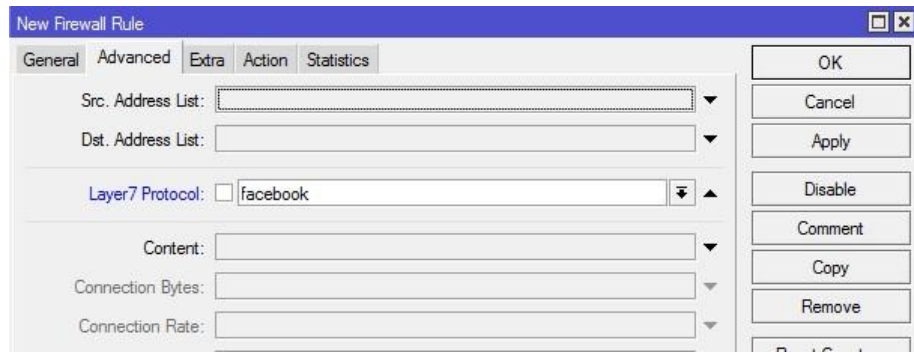


Gambar 2.25 New Firewall Rule untuk Web Proxy L7 Protocols

4. Berpindah pada tab advanced isikan **facebook** pada **Layer 7 Protocols** seperti pada gambar 2.26

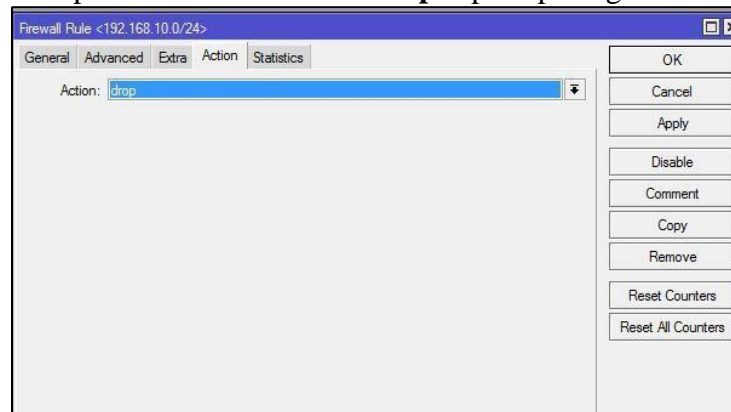


Praktikum Management Jaringan



Gambar 2.26 Advanced Tab New Rule Firewall untuk Web Proxy L7 Protocols

5. Berpindah pada **tab action** isikan **drop** seperti pada gambar 2.27

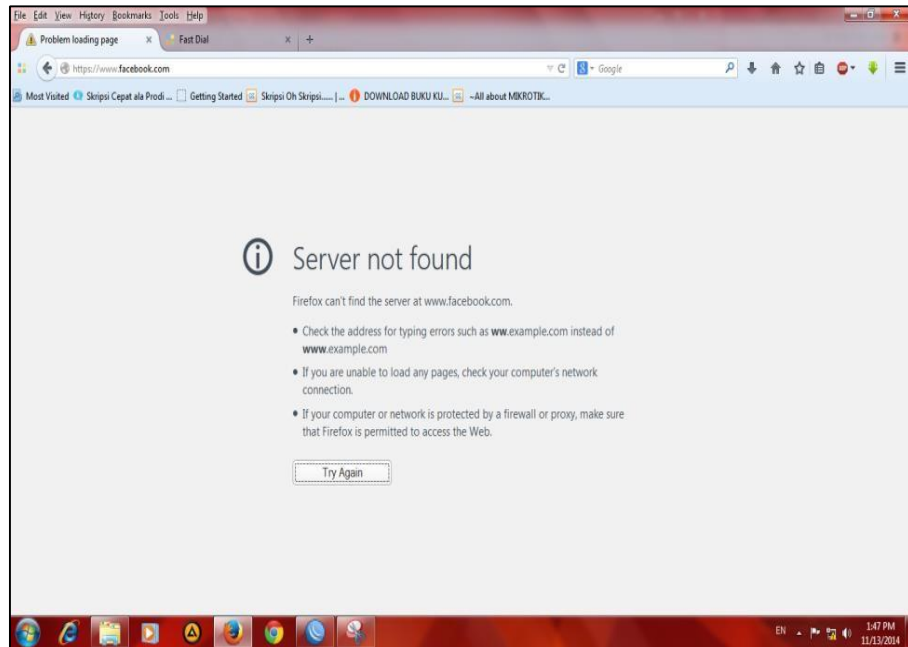


Gambar 2.27 Action Tab New Rule Firewall untuk Web Proxy L7 Protocols



Praktikum Management Jaringan

6. Pengujian dapat dilakukan melalui web browser seperti pada gambar 2.28



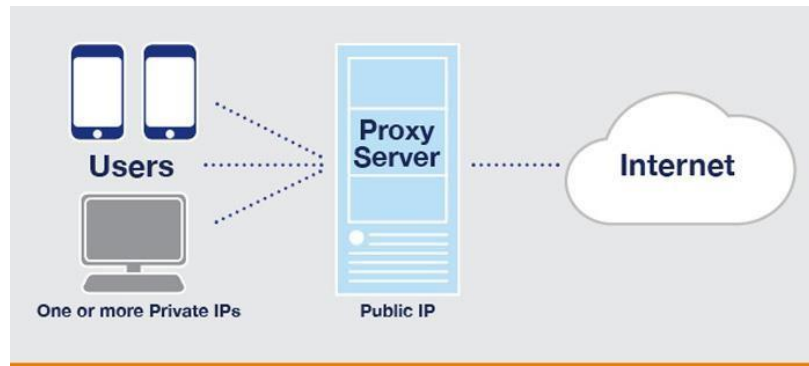
Gambar 2.28 Hasil pengujian web proxy L7 protocols



BAB III PROXY

3.1. Proxy

Proxy adalah suatu aplikasi yang menjadi perantara antara client dengan server, sehingga client tidak akan berhubungan langsung dengan server-server yang ada di Internet. Mikrotik memiliki fitur Web proxy yang bisa digunakan sebagai proxy server yang nantinya akan menjadi perantara antara browser user dengan web server di Internet.



Gambar 2.16 Ilustrasi Web Proxy

3.1.1. Cara Kerja Web Proxy

Ketika user membuka suatu situs, maka browser akan mengirimkan HTTP request ke Server, namun karena computer user ini menggunakan web proxy maka proxy akan menerima HTTP request dari browser tersebut kemudian membuat HTTP request baru atas nama dirinya. HTTP request baru buatan Proxy inilah yang diterima oleh Server kemudian Server membalas dengan HTTP Response dan diterima oleh Proxy yang kemudian diteruskan ke browser user yang sebelumnya melakukan request.

3.1.2. Perbedaan Web Proxy dengan NAT

Mungkin penjelasan cara kerja web proxy di atas hampir mirip dengan NAT (Network Address Translation) Masquerade namun sebenarnya berbeda. Karena jika menggunakan NAT, maka Mikrotik hanya akan meneruskan HTTP Request yang dibuat oleh computer user. HTTP request tersebut diteruskan ke Server oleh



Praktikum Management Jaringan

Mikrotik tanpa membuat HTTP request baru seperti halnya pada Web Proxy. NAT hanya menangani paket data saja, sedangkan Proxy bekerja dengan memeriksa konten dari HTTP Request dan Response secara detail, sehingga Proxy sering juga disebut sebagai Application Firewall.

3.1.3. Keuntungan menggunakan Web Proxy

Fungsi dari proxy secara umum adalah sebagai Caching, Filtering, dan Connection Sharing. Semua fungsi ini dapat anda temui pada Web Proxy Mikrotik.

Berikut ini adalah Keuntungan / Manfaat Web Proxy pada Mikrotik :

a) Caching

Web Proxy Mikrotik dapat melakukan caching content yaitu menyimpan beberapa konten web yang disimpan di memori Mikrotik. Konten tersebut akan digunakan kembali apabila ada permintaan pada konten itu lagi. Misalnya anda membuka Facebook.com, maka file-file pada web tersebut seperti image, script, dll akan disimpan oleh web proxy, sehingga jika lain kali anda membuka Facebook maka tidak perlu konek ke Internet pun halaman itu bisa dibuka dengan mengambil file dari cache proxy. Hal ini dapat menghemat bandwidth Internet dan mempercepat koneksi.

b) Filtering

Dengan menggunakan Web Proxy anda dapat membatasi akses konten-konten tertentu yang di-request oleh client. Anda dapat membatasi akses ke situs tertentu, ekstensi file tertentu, melakukan redirect (pengalihan) ke situs lain, maupun pembatasan terhadap metode akses HTTP. Hal tersebut tidak dapat anda lakukan jika hanya menggunakan NAT.

c) Connection Sharing

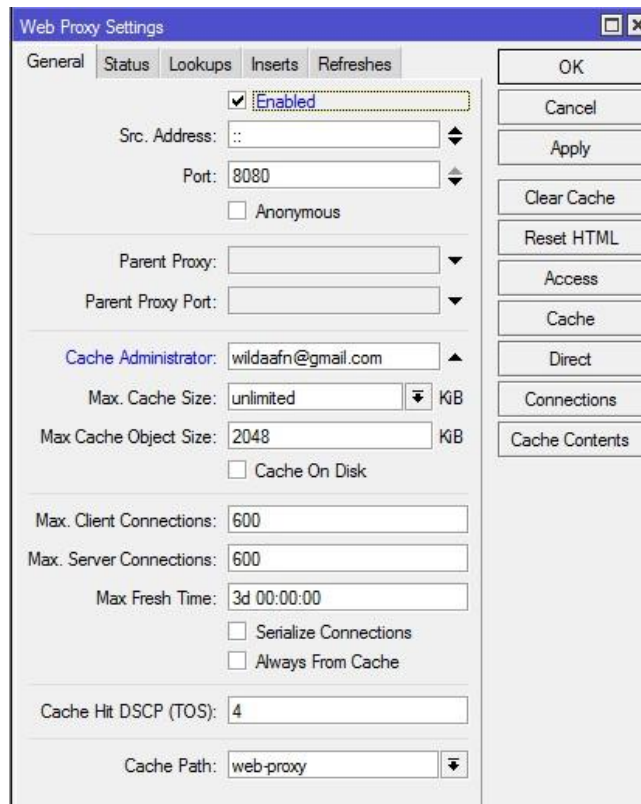
Web Proxy meningkatkan level keamanan dari jaringan anda, karena computer user tidak berhubungan langsung dengan web server yang ada di Internet.



Praktikum Management Jaringan

3.1.4. Konfigurasi Web Proxy

1. Langkah pertama adalah pengaturan Pengaturan Admin Prozy dan port. Klik menu **IP – WEB Proxy**. Kemudian akan muncul window seperti pada gambar 2.17. Setting **Enabled**, port : **8080**, **Cache Administrator : email** dan pengaturan lain sesuai gambar 2.17. klik **Apply – OK**.

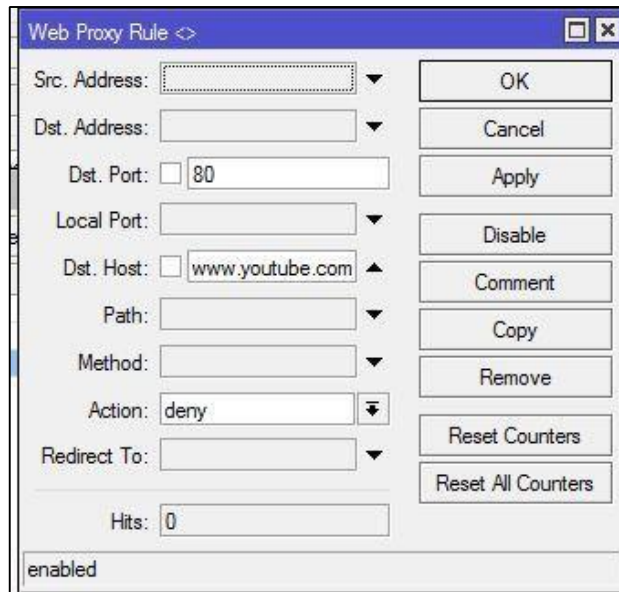


Gambar 2.17 Web Proxy Settings

2. Kemudian tambahkan web atau situs yang akan diblock. Klik **access** pada **web proxy settings** Misal port **HTTP** yaitu **80** untuk **Dst.Host** : www.youtube.com dengan **action deny**. Seperti pada gambar 2.18.

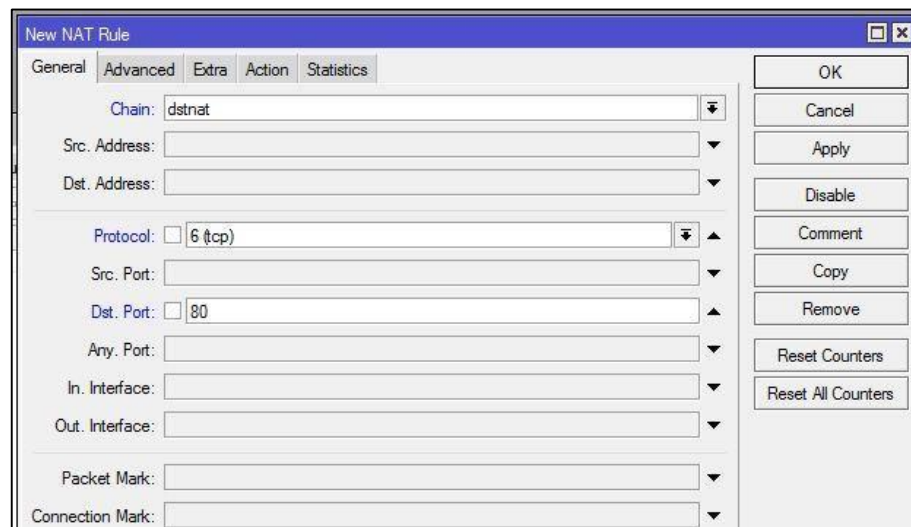


Praktikum Management Jaringan



Gambar 2.18 Web Proxy Rule

3. Disinilah kita akan melakukan penambahan **NAT Rule**. Klik **IP – FIREWALL**. Kemudian tambahkan rule nat baru pada **tab general** seperti pada gambar 2.19

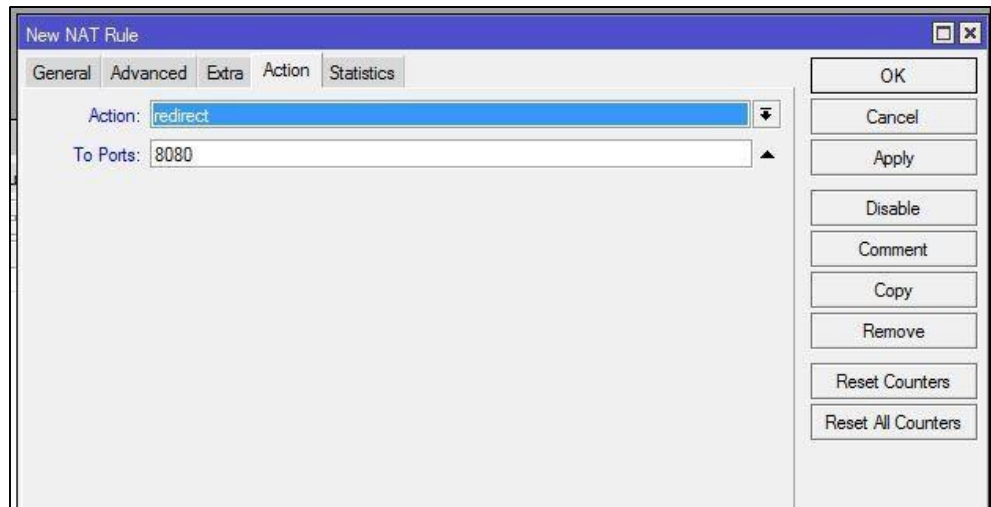


Gambar 2.19 Membuat New Rule NAT untuk web prox

4. Berpindah pada **tab action** pilih **redirect** dan dipindahkan ke port **8080** seperti pada gambar 2.20. klik **Apply – OK**

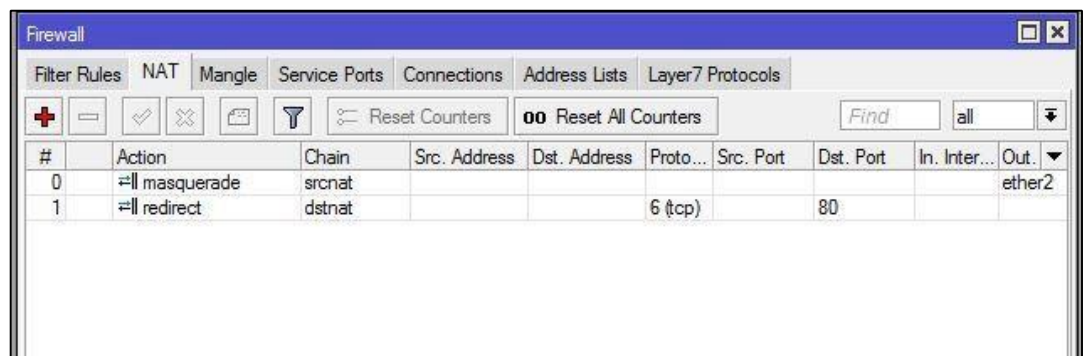


Praktikum Management Jaringan



Gambar 2.20 Action Tab New Rule NAT untuk web proxy

- Setelah disimpan maka akan nampak hasil dari pembuatan rule yang baru untuk web proxy seperti pada gambar 2.21

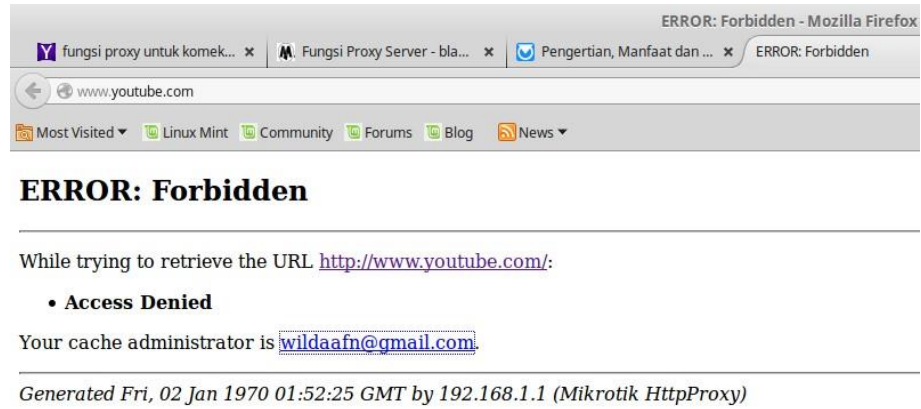


Gambar 2.21 Hasil dari New Rule NAT untuk web proxy

- Lakukan pengujian untuk memastikan bahwa website <http://www.youtube.com> tidak dapat diakses. Seperti pada gambar 2.22.



Praktikum Management Jaringan



Gambar 2.22 Hasil pengujian pada web browser



BAB IV MANAJEMEN BANDWIDTH

4.1 Pengantar *Bandwidth*

Bandwidth bisa berarti jumlah konsumsi paket data per satuan waktu dinyatakan dengan satuan “Bps” (*bit per second*). *Bandwidth* internet disediakan oleh *provider* internet dengan jumlah tertentu tergantung sewa pelanggan. Dengan QoS (Quality of Service) dapat diatur agar *user* tidak menghabiskan *bandwidth* yang di sediakan oleh provider. Istilah *bandwidth* muncul dari bidang teknik elektro, dimana *bandwidth* mempresentasikan jarak keseluruhan atau jangkauan di antara sinyal tertinggi dan terendah pada kanal (*band*) komunikasi.

Pada dasarnya *bandwidth* mempresentasikan kapasitas dari koneksi, semakin tinggi kapasitas, maka umumnya akan diikuti oleh kinerja yang lebih baik, meskipun kinerja keseluruhan juga tergantung pada faktor-faktor lain, misalnya *latency* yaitu waktu tunda antara masa sebuah perangkat meminta akses ke jaringan dan masa perangkat itu memberi izin untuk melakukan transmisi. Kegunaan Manajemen *Bandwidth* adalah sebagai berikut:

- a) Semua komputer dapat menggunakan internet dengan lancar dan stabil walaupun semua unit komputer menggunakan internet dalam waktu yang bersamaan.
- b) Semua bagian unit komputer mendapatkan *bandwidth* sesuai dengan kebutuhan koneksi internet.
- c) Memaksimalkan *bandwidth* di semua unit komputer.
- d) Membantu admin dalam mengontrol *bandwidth*.



4.2 Cara Setting Manajemen *Bandwidth* di Mikrotik

Setting alokasi *bandwidth* terdapat dua jenis yang disediakan oleh Winbox adalah sebagai berikut.

a. *Simple queue*

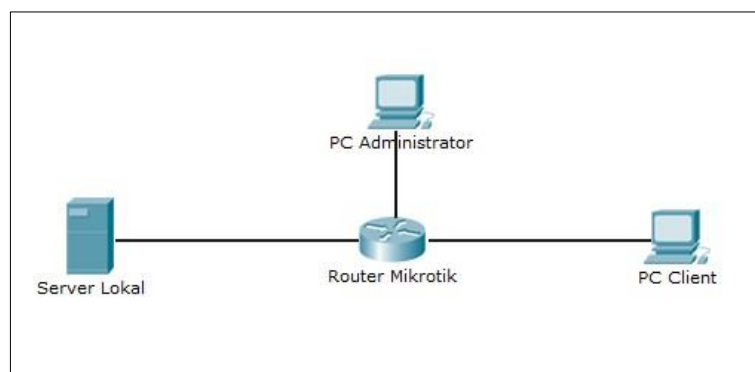
Ketentuan pengaturan *bandwidth* ini cukup sederhana, besarnya *bandwidth* bersifat *fixed* atau sudah disediakan yaitu 64k, 128k, 512k, 1M, dan 2M.

b. *Queue tree*

Merupakan pembagian *bandwidth* yang membawahi beberapa kelas. Sebelum membuat *queue tree* perlu dibuat *mangle* (untuk membuat *mark connection* dan *mark packet*) yang berfungsi untuk memonitor koneksi dan paket yang dilewatkan.

Namun dalam bab ini yang akan dibahas adalah *simple queue*. Mengapa *simple queue*? “karena sebelum belajar *queue tree* harus mengerti *simple queue*, selain itu *simple queue* juga merupakan setting alokasi *bandwidth* yang sangat ringan dan mudah.”

Gambar 3.1 berikut ini merupakan desain jaringan yang akan dilakukan manajemen *bandwidth*. *Bandwidth* berasal dari mikrotik sehingga client yang akan melakukan download file dari server memiliki kecepatan yang dibatasi.



Gambar 3.1 Desain Jaringan Komputer

Kita akan melakukan manajemen *bandwidth* dengan menggunakan Mikrotik. Berikut ini adalah langkah-langkah yang digunakan untuk melakukan manajemen Bandwith.



Praktikum Management Jaringan

1. Langkah awal kita harus *login* sebagai administrator ke dalam mikrotik. Pada Gambar 3.2 berikut ini merupakan tampilan login mikrotik. Kita klik pada *Connect*.



Gambar 3.2 Login Mikrotik

2. Langkah selanjutnya kita tambahkan dulu IP *address* pada setiap *port* yang ada. Kita masuk ke *menu "IP"* lalu pilih *address*. *Menu* tersebut kita pilih tombol "+" atau "*plus*". Setelah itu kita masukkan IP pada *port* yang ke 2 sebagai jalur ke komputer *client*.

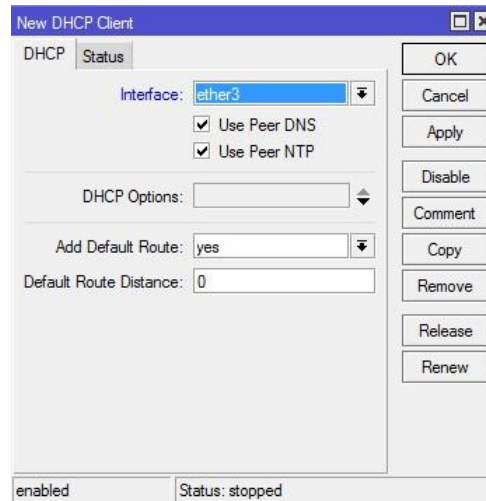


Gambar 3.3 Setting IP Port 2



Praktikum Management Jaringan

- Langkah berikutnya kita *menu “IP”* lagi dan pilih *DHCP Client* dan pilih tombol “+”. Pada langkah ini adalah kita akan meminta IP *public* pada ISP (*Internet Service Provider*) yang akan di gunakan untuk menyambungkan internet ke IP Lokal. Pada gambar 3.4 terlihat *interface* menunjukkan ether3 atau port ke 3, karena pada *port* itulah kita menyambungkan internet dari IP *Public*.

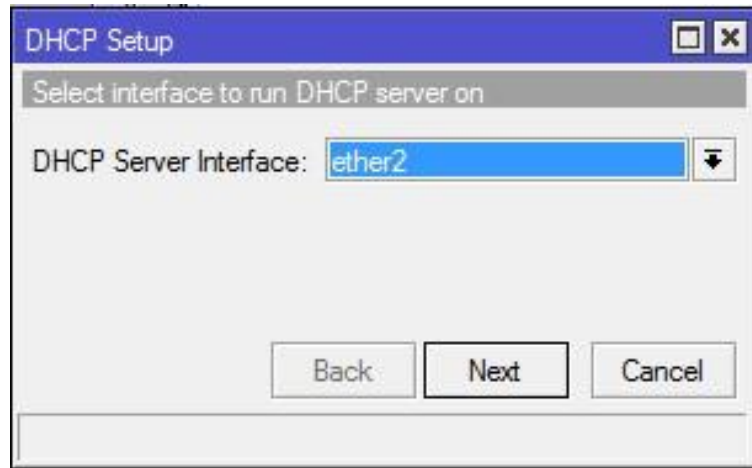


Gambar 3.4 Setting IP DHCP Client pada port 3

- Pada langkah ini kita akan membuat sebuah *DHCP Server* dimana *client* yang menyambung pada router ini akan mendapatkan IP *Address* secara dinamis, jadi nantinya setiap *client* tidak harus menkonfigurasi IP *address*-nya satu-persatu. Kita pilih *menu “IP”* lalu klik *DHCP Server*. Pada *menu DHCP Server* klik saja “*DHCP Setup*” kemudian akan muncul beberapa langkah seperti :
 - DHCP Server Interface* adalah kita harus menentukan *port* mana yang akan di gunakan untuk *client*. Pada gambar 3.5 ether2 atau *port* ke 2 lah yang akan di gunakan untuk *client*. Jika sudah klik Next.

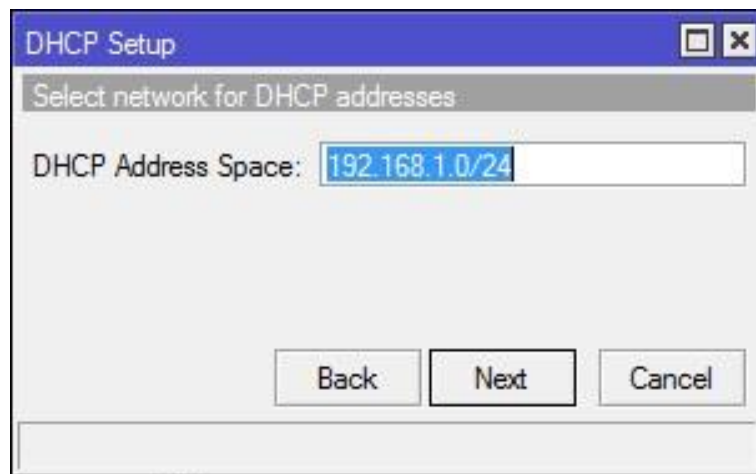


Praktikum Management Jaringan



Gambar 3.5 Konfigurasi DHCP Server 1

- b) Berikutnya kita konfigurasi DHCP *Address Space* dimana IP Address yang akan kita tulis adalah IP Address Network. Di gambar 3.6 dituliskan 192.168.0/24 karna IP Address Client yang akan tersambung dengan router tersebut *host*-nya adalah 0-255.

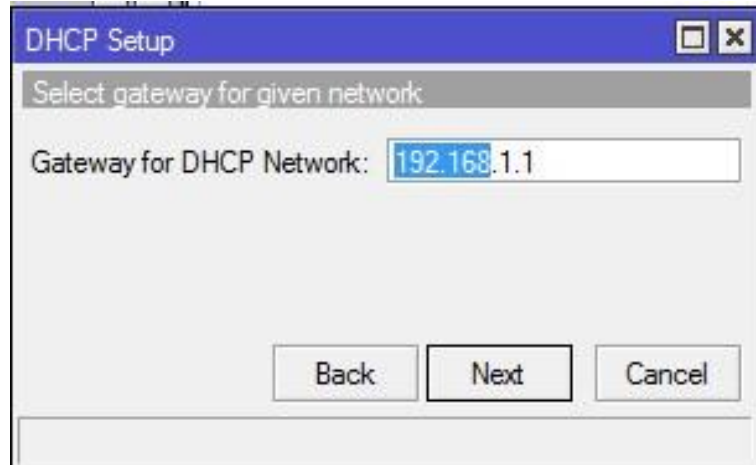


Gambar 3.6 Konfigurasi DHCP Server 2

- c) Kemudian adalah kita akan mengkonfigurasi IP Address Gateway untuk jaringan DHCP, pada gambar 3.7 IP Address Gateway-nya adalah 192.168.1.1 karena IP Address tersebut adalah IP Address dari router yang kita gunakan juga.

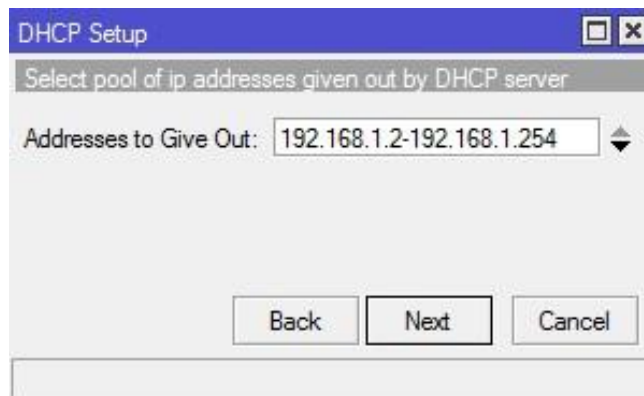


Praktikum Management Jaringan



Gambar 3.7 Konfigurasi DHCP Server 3

- d) Selanjutnya kita akan mengkonfigurasi jarak dari *Host IP Address* berapa sampai *Host IP Address* berapa yang akan di terima oleh *client* yang menyambung ke router kita. Pada gambar 3.8 jarak *IP Address* yang di isikan adalah 192.168.1.2-192.168.1.254, jadi komputer yang menyambung ke router kita akan mendapatkan satu *IP Address* yang acak dari *IP Address* 192.168.1.2 sampai 192.168.1.254.



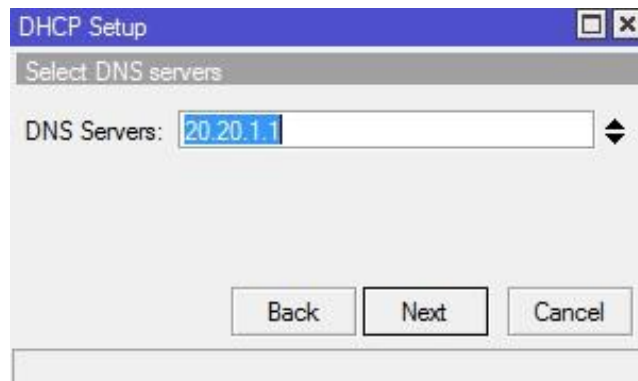
Gambar 3.8 Konfigurasi DHCP Server 4

- e) Setelah itu kita akan mengisi DNS (*Domain Name Server*), DNS ini sudah langsung di isi secara otomatis dan karena sudah di dapatkan dari ISP. Jika



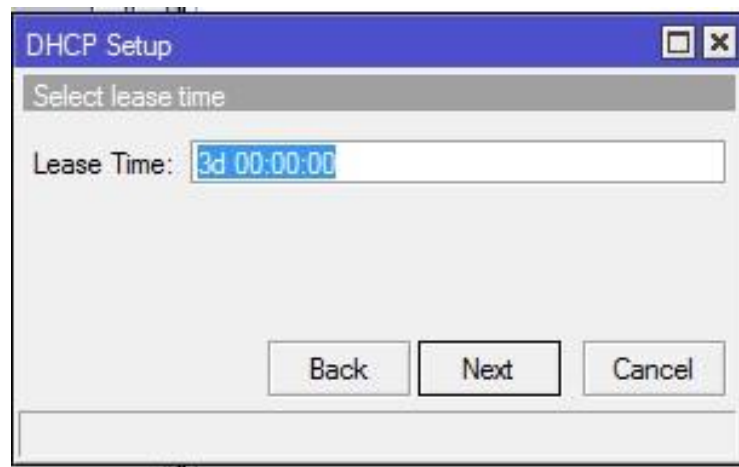
Praktikum Management Jaringan

kalian ingin menambahkannya juga bisa dengan cara klik tombol segitiga yang ke mengarah ke bawah lalu tuliskan DNS yang kalian inginkan.



Gambar 3.9 Konfigurasi DHCP Server 5

- f) Untuk langkah terakhir ini kita akan memasukkan berapa waktu yang kita *setting* untuk pembaruan IP Address bagi *client*. Pada gambar 3.10 di atur 3d 00.00.00, jadi jika DHCP Server sudah di gunakan selama 3 hari, maka setiap *client* yang menyambung nantinya IP Address-nya akan berubah lagi.



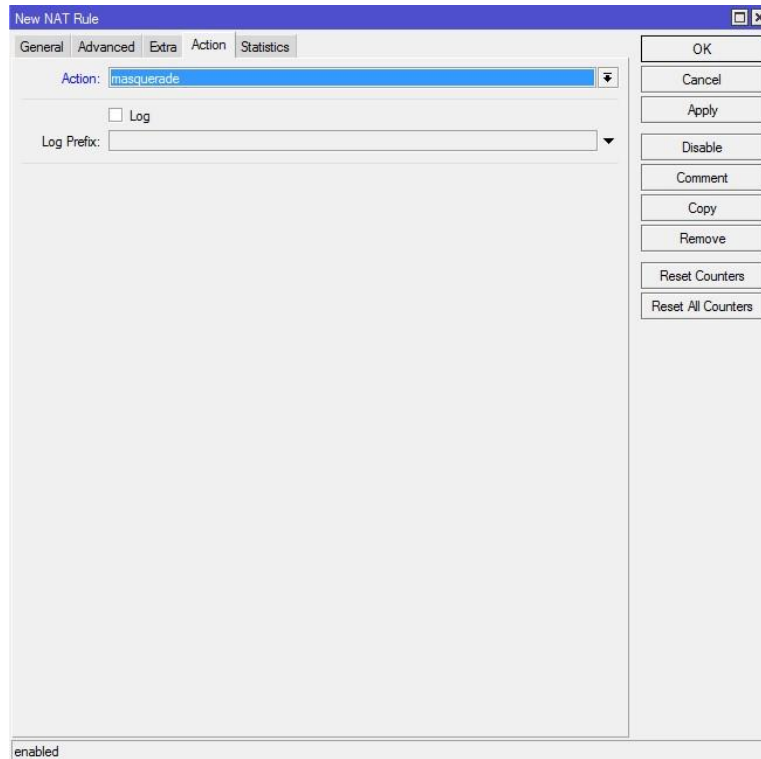
Gambar 3.10 Konfigurasi DHCP Server 6

5. Langkah selanjutnya kita *setting* NAT (*Network Address Translation*) yaitu penerjemahan IP Address Publik ke IP Address Lokal agar komputer yang mendapatkan IP Lokal dapat mengakses IP Publik yaitu internet. Pilih *menu*



Praktikum Management Jaringan

“IP” lalu *Firewall*, pada sub-menu pilih NAT dan klik tanda “+”. Di menu *New NAT Rule* pilih sub-menu *Action* dan pilih *Masquerade*. Pada *Action Masquerade* itulah penerjemahan IP Address Publik ke IP Address Lokal di lakukan.

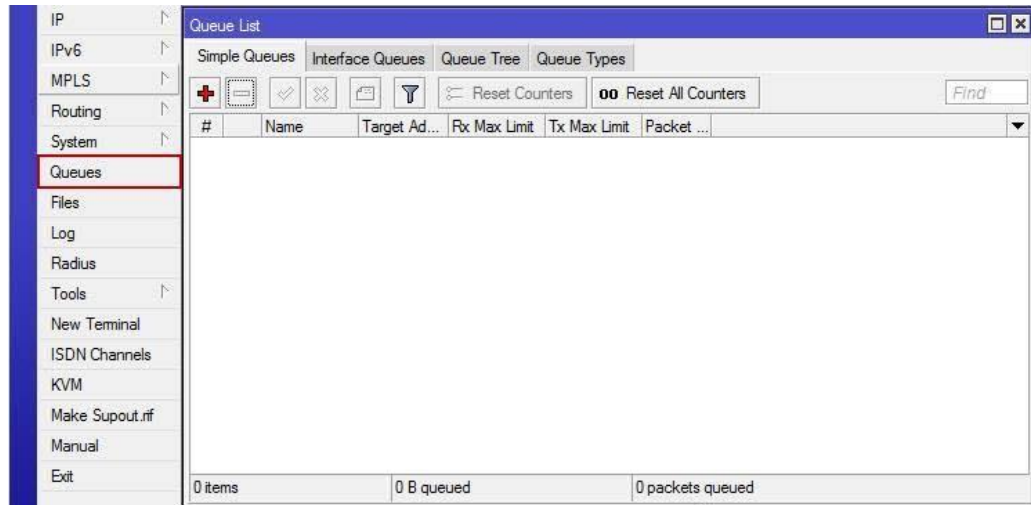


Gambar 3.11 Konfigurasi NAT

- Langkah selanjutnya bila telah masuk kedalam winbox adalah membuka pada menu *Queues* untuk mengatur *bandwidth* seperti pada Gambar 3.12.

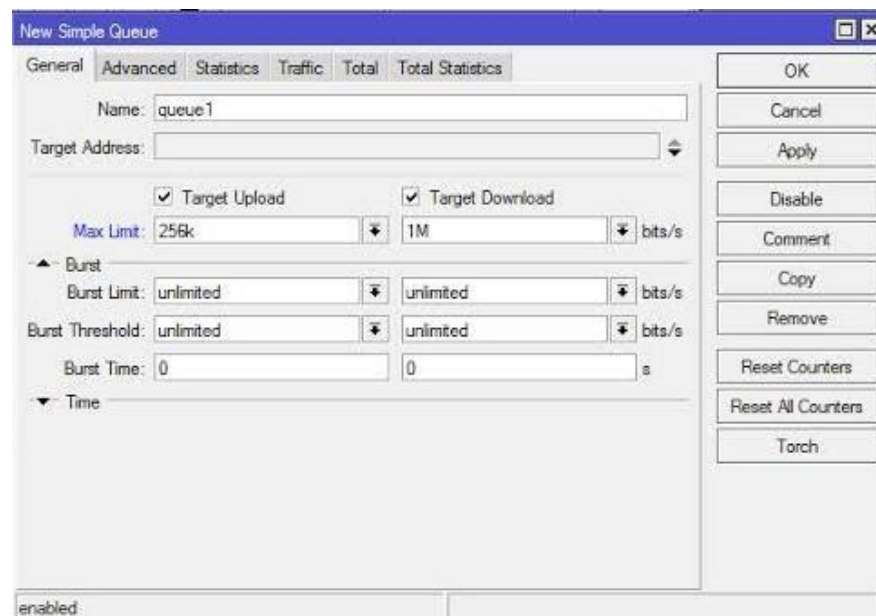


Praktikum Management Jaringan



Gambar 3.12 Membuka Menu Queue

7. Selanjutnya pilih tanda “+” untuk menambah *rule* pada *Queue List*. Maka akan muncul tampilan seperti pada Gambar 3.13 berikut ini.



Gambar 3.13 Setting Simple Queue Untuk Keseluruhan

Dalam melakukan setting simple queue yang perlu disetting adalah

- Name : Diisikan sesuai dengan nama yang dikehendaki
- Target Address : Diisi dengan alamat IP Address PC tujuan yang akan di *limit bandwidth*-nya. Jika untuk keseluruhan maka diinputkan *Network Address* dan



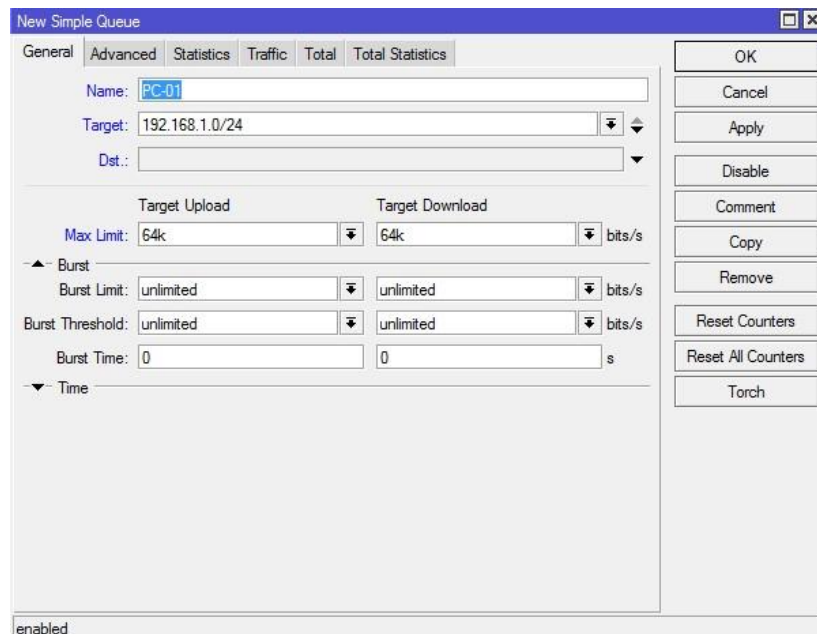
Praktikum Management Jaringan

Prefix length-nya. Sedangkan untuk melakukan *limit* pada PC tertentu. Diinputkan IP Address PC tersebut.

- Target Upload : Menentukan maksimal *limit* untuk *upload* ?
Target Download : Menentukan Maksimal *limit* untuk *download*-nya

Setelah selesai, klik *Apply* dan kemudian OK .

8. Berikut ini pada Gambar 3.14 merupakan cara setting *limit Bandwidth* untuk PC *target*. Langkah pertama adalah dengan setting pada *General*.

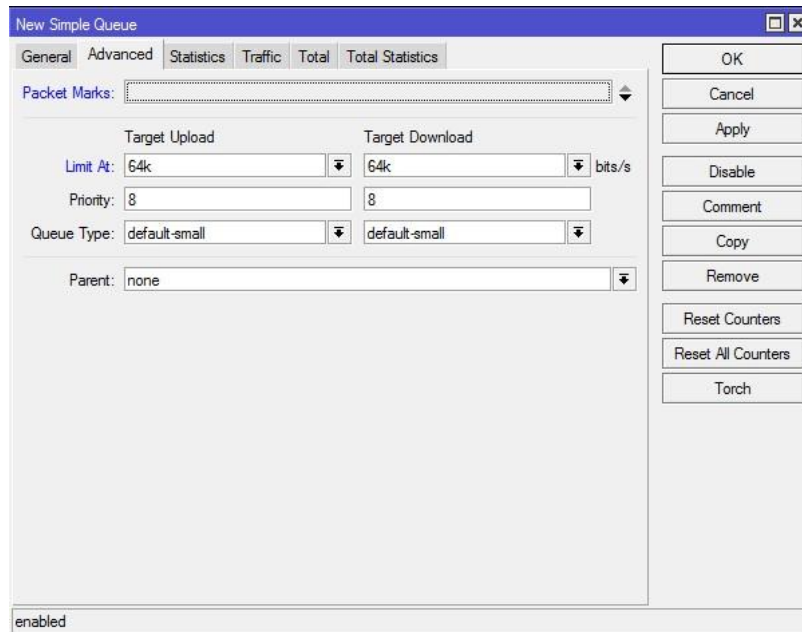


Gambar 3.14 Setting General Limit Bandwidth PC

9. Setelah itu melakukan setting pada *Advanced* seperti pada Gambar 3.15 berikut ini.

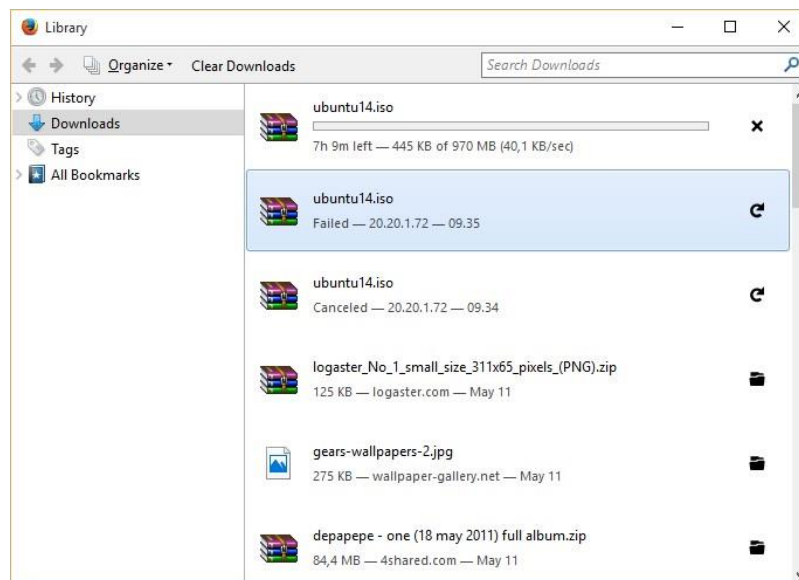


Praktikum Management Jaringan



Gambar 3.15 Setting Advanced Limit Bandwidth PC

10. Setelah melakukan *limit bandwidth* adalah melakukan *testing* dengan *download file* pada jaringan lokal. Berikut ini adalah tampilan hasil dari limit bandwidth yang telah dilakukan.



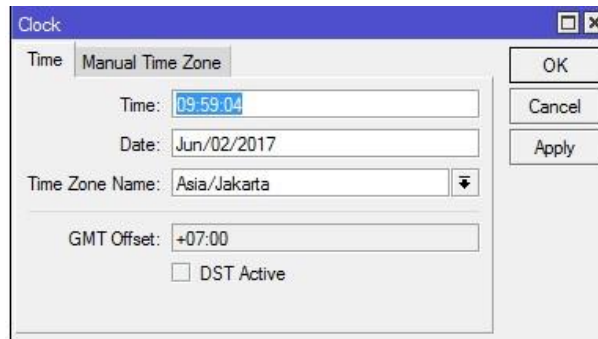
Gambar 3.16 Hasil Dari Limit Bandwidth.



Praktikum Management Jaringan

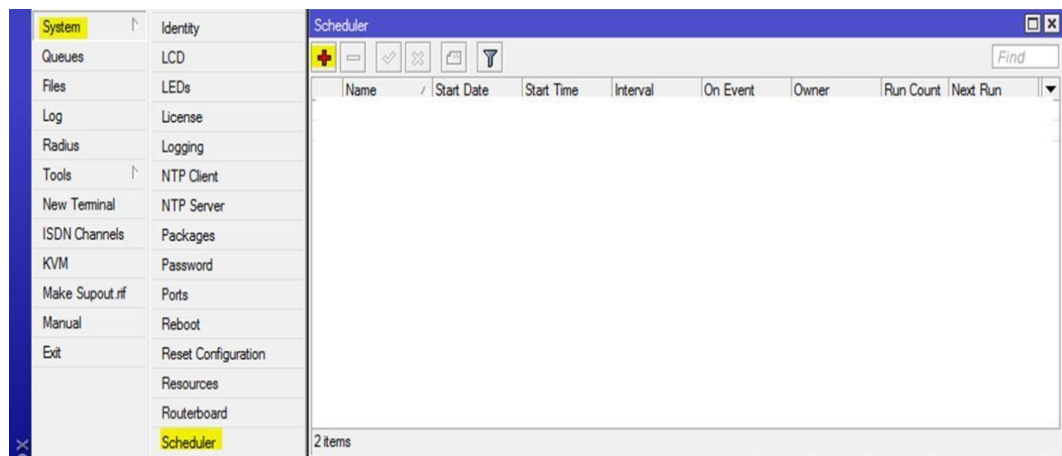
4.3 Schedule Task Mikrotik

Pengaturan otomatis pada mikrotik untuk melakukan penjadwalan suatu perintah yang akan dieksekusi sesuai jadwal yang telah ditentukan. *Scheduler* bisa dimanfaatkan untuk me-reboot otomatis mikrotik, melakukan blokir situs pada jam-jam tertentu yang tentunya sangat membantu untuk mengatur jaringan computer. Pada contoh di bawah kita melakukan proses *booting* secara berkala.



Gambar 3.17 tampilan konfigurasi clock

Selanjutnya klik menu “System” lalu pilih “Scheduler” seperti pada gambar 3.18.



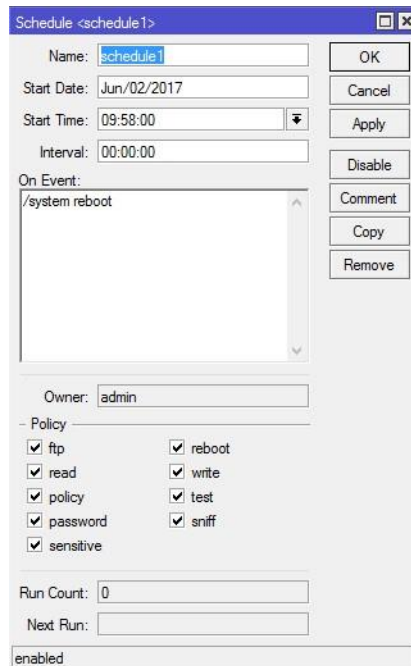
Gambar 3.18 tampilan Scheduler

Klik tanda “+” pada jendela *scheduler*, dan isikan penjadwalan yang anda inginkan dan jangan lupa pada kolom “On Event” isikan “/system reboot” sebagai perintah untuk *reboot*.

Pada contoh di berikut, Router Mikrotik di setting agar *reboot* setiap hari pada jam 09:58:00 seperti pada gambar 3.14.



Praktikum Management Jaringan



Gambar 3.14 tampilan pengisian nama schedule

- **Name** : Nama penjadwalan yang anda inginkan
- **Start Date** : Tanggal dimulainya penjadwalan tersebut dimulai, secara otomatis akan tertulis tanggal hari ini mikrotik di *reboot* secara otomatis oleh *system*.
- **Interval** : *Interval* / jangka waktu penjadwalan, dalam kasus ini setiap berapa jam / hari router akan di restart, dalam contoh interval-nya 1d (satu hari) yang artinya, penjadwalan akan di eksekusi 1 hari setelah penjadwalan pertama dieksekusi, sederhananya setiap hari pada jam 00:00 Router Mikrotik dijadwalkan untuk *reboot*
- **On Event** : Kolom yang berisi “perintah” atau “*script*” yang harus dieksekusi dalam penjadwalan. Dalam kasus ini adalah script/perintah untuk *reboot*, maka di isi dengan “/system reboot”



BAB V MANGLE

5.1 Pengantar Firewall (Mangle)

Mangle merupakan salah satu fitur pada firewall router mikrotik yang digunakan untuk memberi tanda (*mark*) pada paket data, kadang pekerjaan memberi tanda ini disebut dengan *marking* tujuan dari pemberian tanda ini adalah agar packet lebih mudah dikenali lagi yang akhirnya lebih memudahkan anda menerapkan filter masquerade, routing maupun pada saat anda melakukan management bandwidth,

Penggunaan mangle ini sebenarnya bisa dilakukan oleh NAT saja namun akan sangat merepotkan bila menggunakan NAT di banding menggunakan mangle dalam management jaringan,

Dalam menggunakan fitur mangle dengan benar anda harus mengetahui arah tujuan dari packet data, jenis-jenis *protocol*, penggunaan *source /destination port*, maupun *connection state* dari suatu packet data secara singkatnya modal yang digunakan untuk menerapkan *firewall filter* di terapkan pula pada saat menerapkan *firewall mangle*

tanda atau marking yang digunakan pada packet data hanya di baca dan digunakan pada router yang bersangkutan, marking tersebut akan di lepas pada saat packet akan meninggalkan router, sehingga marking pada suatu router tidak dapat di gunakan pada router lainnya. Firewall mangle juga nantinya akan terdiri dari susunan rule rule, yang sama seperti firewall filter maupun NAT, rule rule tersebut juga nantinya kan dibaca secara berurutan dari atas ke bawah: ada tiga jenis marking yang digunakan yaitu :

- a) Connection mark
- b) Packet Mark
- c) Route mark

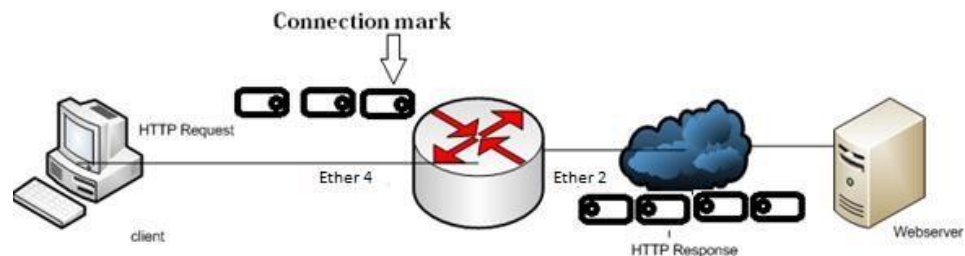


Praktikum Management Jaringan

5.1.1 Connection mark

Connection mark merupakan jenis marking yang di gunakan untuk menandai adanya suatu koneksi, yang kita tahu ketika sebuah *computer* berkomunikasi akan mengeluarkan serangkaian packet (*data stream*) *Connection mark* berfungsi memberi tanda packet yang pertama kali keluar dari computer tersebut.

Connection mark dapat di gunakan untuk memberikan tanda (marking) pada packet pertama, baik request dari client maupun packet pertama yang merupakan reponse dari server



Gambar.5.1 connection mark

Pada gambar 5.1 terlihat sebuah client yang melakukan browsing ke sebuah webserver di internet yang pertama kali dikeluarkan oleh client adalah sebuah packet HTTP Request yang bertujuan meminta sebuah halaman html pada webserver pada packet request ini terdapat 3 buah paket pada proses ini connection mark berfungsi untuk memberikan tanda dari packet pertama tidak untuk packet selanjutnya adapun packet selanjutnya adalah tugas dari packet mark.

Bila menggunakan gambar acuan pada gambar 5.1

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 action=mark-connection new-connection-mark=koneksi
```



Praktikum Management Jaringan

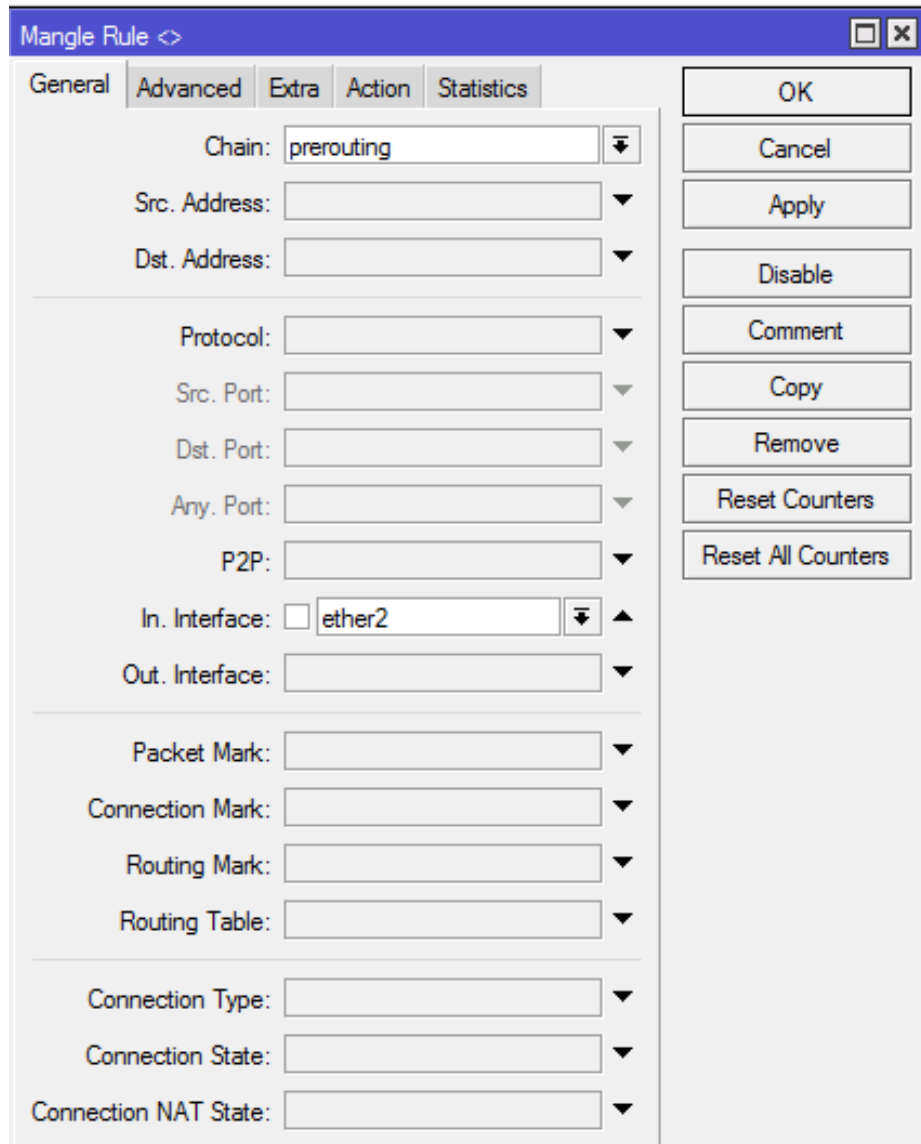
Parameter yang perlu anda lihat adalah in-interfaces yang menggunakan ether 2 ini karena HTTP request yang keluar dari client yang menuju internet yang akan masuk.pada router pada interfaces ether 2 para meter passtrough yang di gunakan adalah yes.

Begitu juga dengan parameter chain pre routing, chain ini di pilih karena merupakan chain yang di gunakan untuk melakukan marking bagi paket yang di tujukan untuk router atau paket yang melintasi router, chain prerouting juga merupakan chain yang mangijinkan penggunaan parameter in-interfaces, anda tidak bisa menggunakan chain pre routing karena post routing tidak mengijinkan anda memilih parameter in-interfaces dengan menggunakan winbox, anda dapat melakukan melalui IP > firewall>tab mangle >tombol add (+)

Seperti gambar di bawah ini 5.2



Praktikum Management Jaringan



Mangle Rule <>

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: ☐ ether2

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

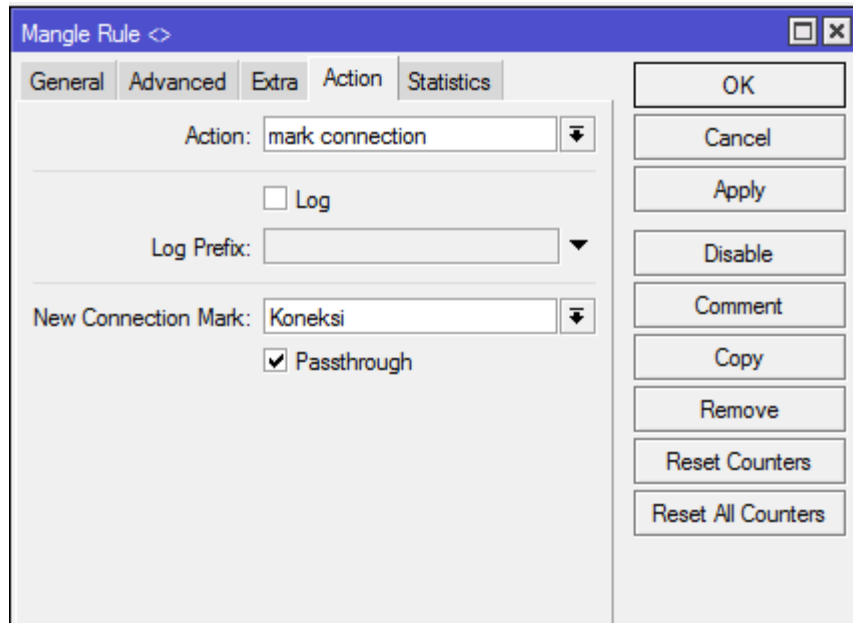
Reset All Counters

Gambar.5.2 connection mark untuk traffic

Sedangkan untuk action dapat dilakukan pada tab action seperti pada gambar berikut ini yang di mana pada langkah ini kita mengisi tindakan action mark paket pada client yang telah kita buat sebelumnya. adapun pengisianya seperti pada gambar 5.3



Praktikum Management Jaringan



Gambar.5.3 pengisian action mark connection

Untuk mengujinya cobalah melakukan browsing ke salah satu situs dan amati hasilnya misal yang kita buka adalah situs www.Google.com kemudian perhatikan counter packet yang di tampilkan oleh winbox.walaupun hanya membuka halaman depan dari google akan terlihat bahwa computer anda telah membuat beberapa koneksi sekaligus (simultan)

The image shows the 'Firewall' configuration window in Mikrotik WinBox, specifically the 'Connections' tab. It displays a table of active connections. The table has columns for '#', 'Action', 'Chain', 'Protocol', 'In. Interface', 'Connection Mark', 'Bytes', and 'Packets'. There are two rows: one for 'Mark Connection' and one for 'mark connection'. The 'mark connection' row shows it is in the 'prerouting' chain, using 'ether2' as the interface, with a connection mark of '2309.5 KIB' and '33 313' packets.

#	Action	Chain	Protocol	In. Interface	Connection Mark	Bytes	Packets
0	mark connection	prerouting	ether2		2309.5 KIB	33 313	

Gambar.5.4 hasil dari conection mark

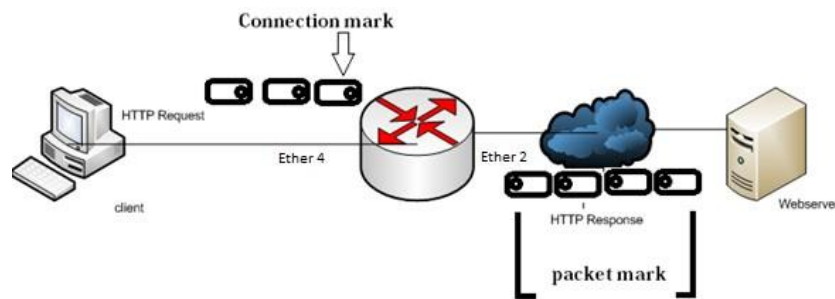


Praktikum Management Jaringan

5.1.2 Packet mark

Setelah sebelumnya membahas tentang connection mark maka saat ini yang akan di bahas adalah packet mark, packet mark adalah sebuah upaya yang dilakukan untuk menandai semua packet yang keluar dan masuk dari sebuah computer client.

Dikarenakan connection mark di gunakan untuk menandai hanya pada packet pertama packet mark di gunakan untuk menandai semua packet yang keluar dan masuk pada pc client itulah kegunaan dari packet mark. Dapat anda ketahui dalam pengiriman data menggunakan TCP/IP data yang di kirimkan akan di pecah pecah sehingga membentuk *stream data*, ilustrasinya seperti pada gambar berikut ini.



Gambar.5.5 gambaran dari mark packet

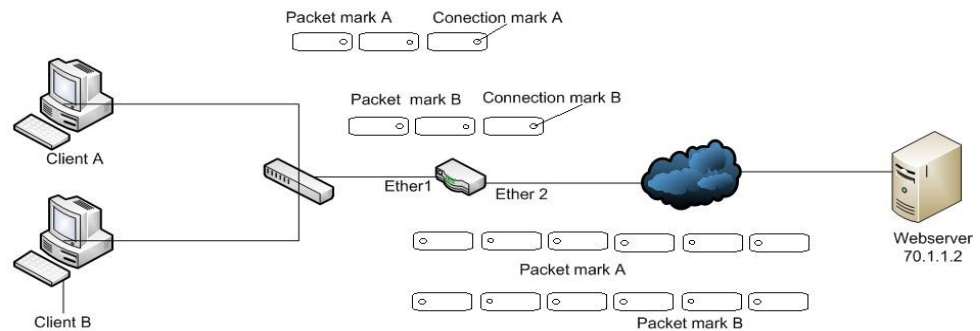
Gambar di atas merupakan sebuah kegiatan dari computer client yang melakukan proses download data dari sebuah webserver di internet di karenakan menggunakan proses TCP/IP maka HTTP melakukan request data yang berisikan permintaan download ke web server, dan HTTP response yang merupakan data file yang di berikan web server di internet. Di karenakan menggunakan TCP/IP maka umumnya suatu proses pengiriman data dilakukan 2 arah , maka anda dapat melihat http request yang berisikan permintaan download ke webserver dan HTTP response yang merupakan data atau file yang diberikan web server ke computer client.itulah mengapa ilustrasi pada gambar di atas menampilkan traffic download



Praktikum Management Jaringan

lebih besar di banding traffic upload I karena proses download rata rata lebih besar daripada proses upload.

Masih pada pembahasan dari gambar di atas mark connection di gunakan untuk menandai packet pertama dan packet mark digunakan untuk menandai packet packet lainnya.



Gambar.5.6 contoh mark packet bila terdapat 2 buah proses data

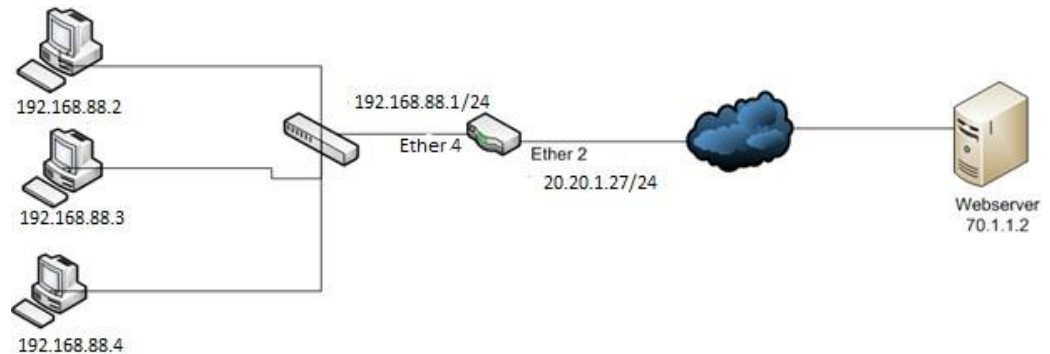
Pada gambar di atas terdapat gambar yang menjelaskan terdapat 2 buah pc *client* yang melakukan *download* dari web server dimana terdapat 2 buat mark packet dan mark connection yang berbeda ,maka bila ingin supaya sekenario gambar di atas benar dengan mark packet yang benar pula maka harus memperhatikan parameter yang di gunakan, bila client A pada awalnya di beri nama mark Connection = Client A-CONN maka parameter sebelumnya haruslah di berikan nama yang sama connection mark=client-A_CONN.anda akan melihat pada penjelasan penjelasan berikutnya.



Praktikum Management Jaringan

Skenario 1

Pada skenario INI ANDA DI HARUSKAN membuat marking pada packet .iso dan .exe (baik upload maupun download) dari semua computer client yang ada pada jaringan 192.168.2.0/24. Tujuan nya adalah untuk memisahkan bandwidth upload/download file .exe dan .iso. anda dapat melihat topologinya sebagai berikut :



Gambar.5.7 marking untuk semua jenis koneksi

Tahap pertama tentunya hal yang harus di buat adalah membuat connection untuk mark untuk membuat marking bagi “semua jenis” koneksi yang di buat oleh semua jenis koneksi yang di buat oleh semua computer client , perintah yang dapat anda gunakan adalah sebagai berikut.

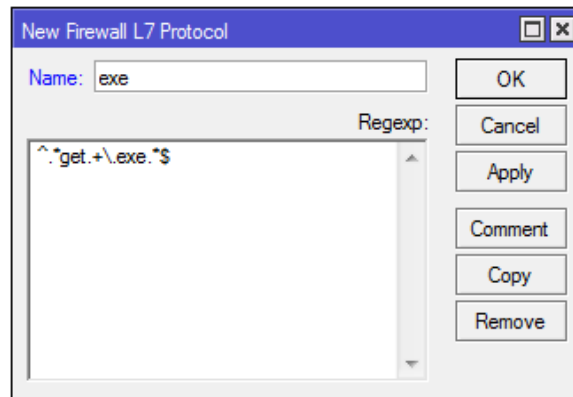
```
[admin@gateway]>ip firewall mangle
Add chain=prerouting action=mark-connection new-connection-mark=Koneksi
passthrough=yes in-interface=ether2
```



Praktikum Management Jaringan

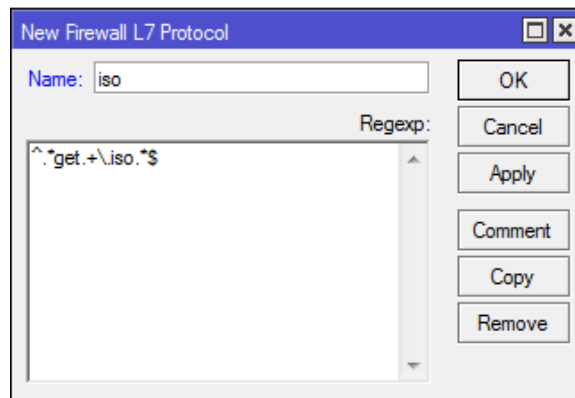
Setelah membuat mark-connection langkah selanjutnya adalah membuat regexp untuk file .iso dan .exe. Untuk setting regexp adalah dengan masuk ke Menu Firewall kemudian pilih Layer7 Protocols. Berikut regexp untuk file .iso dan .exe :

File .exe



Gambar.5.8 Regexp file exe

File .iso



Gambar.5.9 Regexp file iso



Praktikum Management Jaringan

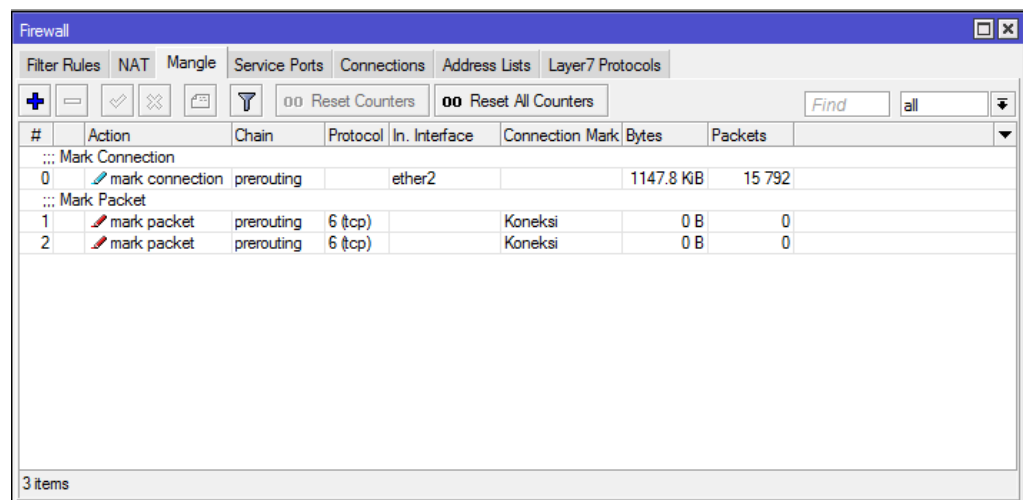
Langkah selanjutnya adalah membuat marking terhadap paket .iso dan .exe untuk keseluruhan traffic upload dan download dengan menggunakan paket mark. yang harus di perhatikan pada konfigurasi ini adalah parameter connection mark menggunakan mark connection yang telah di buat pada tahap pertama, pada langkah ini akan membuat packet mark pada jenis file .iso adapun script yang digunakan adalah sebagai berikut.

```
[admin@gateway]>ip firewall mangle chain=prerouting action=mark-packet  
new-packet-mark=paket_iso passthrough=yes protocol=tcp layer7-protocol=iso  
connection-mark=Koneksi
```

Langkah selanjutnya adalah membuat marking terhadap packet .exe

```
[admin@gateway]>ip firewall mangle add chain=prerouting action=mark-packet  
new-packet-mark=packet_exe passthrough=no protocol=tcp layer7-  
protocol=exe connection-mark=Koneksi
```

Hasil dari konfigurasi di atas akan menjadi seperti gambar berikut :



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the Mangle tab. It displays two rules: 'Mark Connection' and 'Mark Packet'. The 'Mark Connection' rule is active and has a connection mark of 'Koneksi'. The 'Mark Packet' rule is also active and has a connection mark of 'Koneksi'. Both rules are configured for the 'prerouting' chain and the 'ether2' interface. The 'Mark Packet' rule is configured for protocol 'tcp' and layer 7 protocol 'exe'.

#	Action	Chain	Protocol	In. Interface	Connection Mark	Bytes	Packets
0	mark connection	prerouting		ether2		1147.8 KiB	15 792
1	mark packet	prerouting	6 (tcp)		Koneksi	0 B	0
2	mark packet	prerouting	6 (tcp)		Koneksi	0 B	0

Gambar.5.8 Konfigurasi Mark-Connection dan Mark-Packet



Praktikum Management Jaringan

Sehingga hasil akhir konfigurasi marking tersebut dapat di lihat seperti berikut

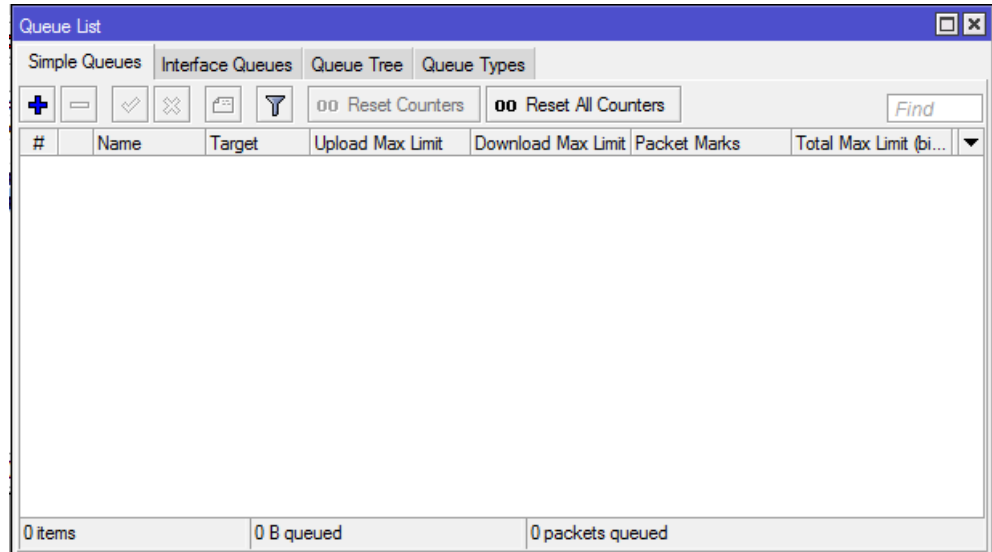
```
[admin@MikroTik] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
0   ;;; Mark Connection
    chain=prerouting action=mark-connection new-connection=
    passthrough=yes in-interface=ether2 log=no log-prefix=""
1   ;;; Mark Packet
    chain=prerouting action=mark-packet new-packet-mark=
    passthrough=yes protocol=tcp layer7-protocol=iso conn
    log=no log-prefix=""
2   chain=prerouting action=mark-packet new-packet-mark=
    passthrough=no protocol=tcp layer7-protocol=exe conn
    log=no log-prefix=""
[admin@MikroTik] >
```

Jika melihat hasil konfigurasi marking di atas, maka keseluruhan traffic upload dan download dari semua computer client di jaringan 192.168.2.0/24 akan dikenal sebagai paket dengan nama “koneksi” perhatikan juga parameter passthrough yang digunakan pada kedua konfigurasi paket mark.



Praktikum Management Jaringan

Langkah selanjutnya adalah memisahkan bandwidth antara file .iso dan .exe dengan menggunakan fitur queue yang ada pada mikrotik. Buka terlebih dahulu menu queue maka akan tampil seperti gambar berikut :



Gambar 5.9. Menu queue

Selanjutnya klik tombol tambah untuk menambah rule pada queue list. Pada general name isi dengan ISP, target isi dengan network address dari client, pada target upload dan download isi dengan 1Mbps/s, kemudian klik apply, Ok seperti pada gambar 5.10 berikut ini



Praktikum Management Jaringan

The screenshot shows the 'New Simple Queue' configuration window. The 'General' tab is selected. The 'Name' field contains 'ISP'. The 'Target' field contains '192.168.2.0/24'. The 'Dst.' field is empty. Under the 'Target Upload' and 'Target Download' sections, the 'Max Limit' is set to '1M' bits/s. Under the 'Burst' section, the 'Burst Limit', 'Burst Threshold', and 'Burst Time' are set to 'unlimited', 'unlimited', and '0' respectively. The 'Time' section is collapsed. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', 'Reset All Counters', and 'Torch'. At the bottom left, the 'enabled' checkbox is checked.

Gambar 5.10 Manegement Bandwidth untuk semua client

Dalam melakukan setting simple queue yang perlu di setting :

Name : di isikan sesuai nama yang di inginkan

Target Address : di isikan dengan alamat ip pc tujuan yang akan di limit bandwidthnya. Jika untuk keseluruhan client maka di inputkan network address dan prefix length nya.

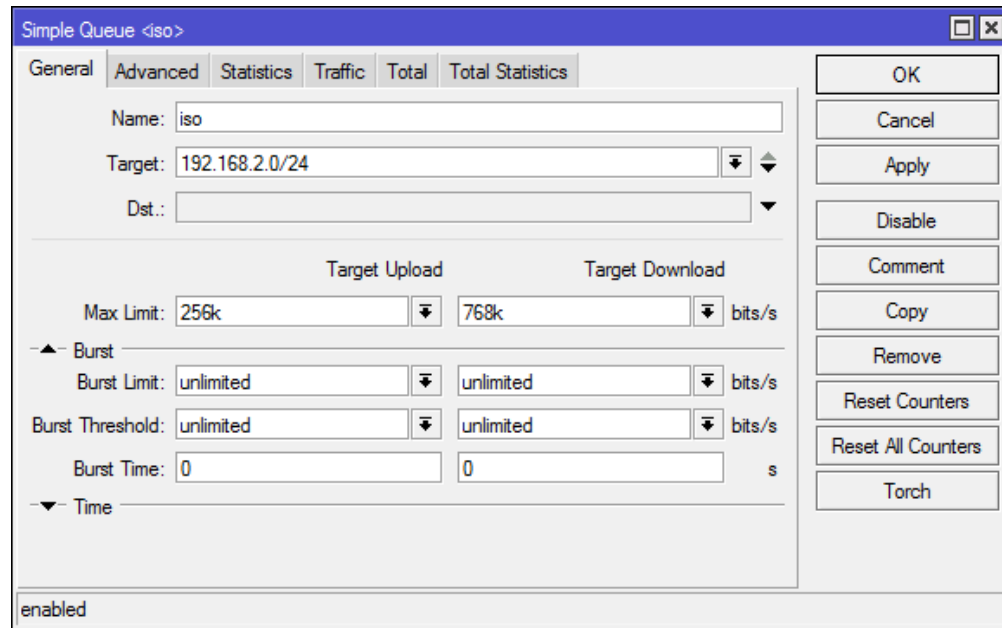
Target upload : menentukan maksimal limit untuk upload

Target download: menentukan maksimal limit untuk download

Kemudian buat queue untuk membagi bandwidth file .iso dan .exe. klik tombol tambah untuk menambah rule. Lakukan konfigurasi seperti pada gambar berikut :

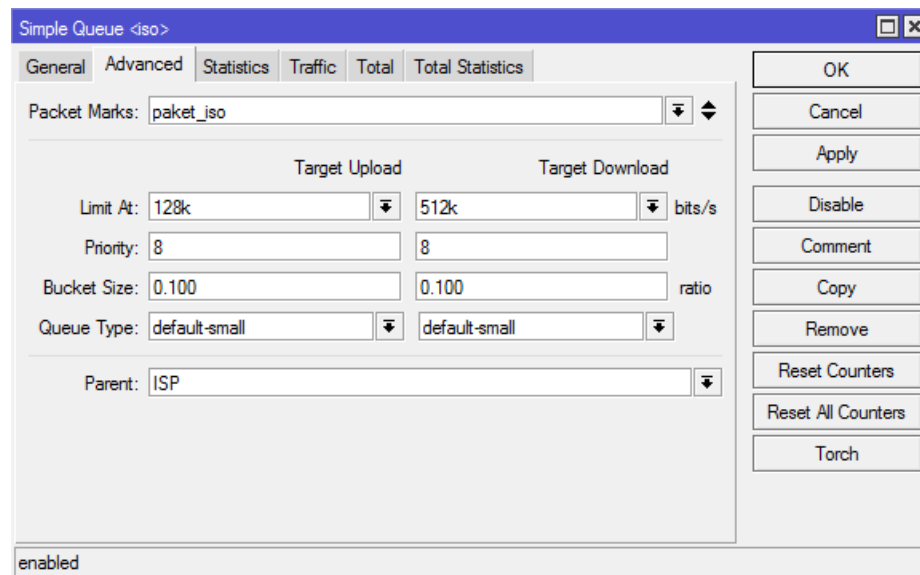


Praktikum Management Jaringan



Gambar 5.11 Management Bandwidth untuk file .iso

Kemudian pindah ke tab Advanced untuk me management bandwidth file iso berdasarkan mark-packet yang telah di buat di awal. Tentukan packet marks sesuai jenis file yang akan delimit. Kemudian isikan limit untuk upload dan download file tersebut.

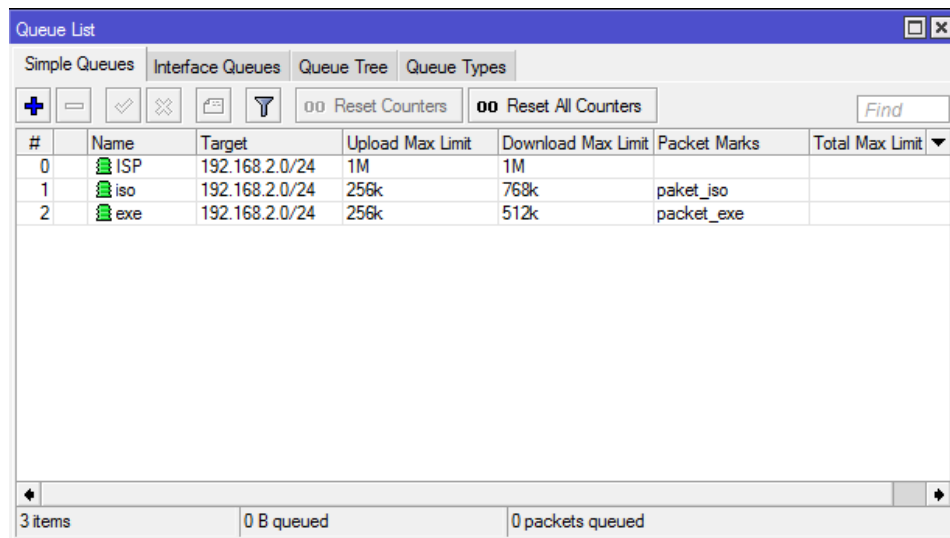


Gambar 5.12 konfigurasi bandwidth file iso berdasarkan mark-packet



Praktikum Management Jaringan

Hasil konfigurasi pada queue bisa dilihat pada gambar berikut ini :



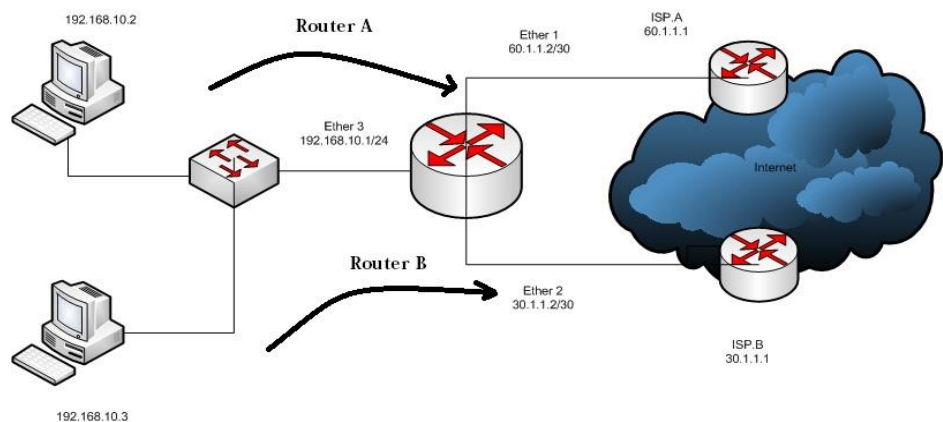
#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit
0	ISP	192.168.2.0/24	1M	1M		
1	iso	192.168.2.0/24	256k	768k	paket_iso	
2	exe	192.168.2.0/24	256k	512k	packet_exe	

3 items 0 B queued 0 packets queued

Gambar 5.13 Konfigurasi pada queue

5.1.3 Route Mark

Route mark adalah jenis marking yang di berikan kepda packet data untuk keperluan routing, hasil dari route mark ini dapat di dimanfaatkan pada saat melakukan konfigurasi default gateway maupun routing static route mark juga di perlukan pada saat melakukan suatu kebijakan atau management routing (policy route) anda dapat melihat gambar 3 berikut ini, jaringan di bawah ini menggunakan 2 buah ISP yang berbeda .



Gambar 5.11 tampilan dari mark routing



Praktikum Management Jaringan

Router gateway di atas ingin memisahkan koneksi internet dari 2 buah computer client yang di miliknya, computer client dengan ip 192.168.10.2 ingin melalui ip A dan client dengan ip dari 192.168.10.3 ingin melalui dari koneksi ISP B bila anda ingin melakukan proses ini anda dapat menggunakan bantuan dari action srcnat.sepeti pada bab sebelumnya namun pada bab ini skenario akan di jalankan dengan menambahkan fitur router mark tentunya harus di konfigurasi terlebih dahulu pada setiap interfaces router gateway.

5.2 Burst

Burst merupakan fitur yang memungkinkan sebuah antrian mendapatkan bandwidth tambahan pada periode waktu tertentu. Bahkan bandwidth yang diperoleh bisa lebih besar dari nilai *max-limit*. tapi sebenarnya ini tergantung dari besarnya bandwidth yang Anda terima dari ISP. Jika Anda berlangganan di kecepatan 1Mbps. Maka maksimal *burst* yang akan diterima ya berkisar bandwith yang anda dapat dari ISP.

Untuk penerapanya langsung saja kita terapkan seperti petunjuk di bawah ini Sebagai contoh kecepatan maksimal jaringan internet Anda 1024kbps, lama waktu *burst* yang diberikan 10 detik, waktu yang digunakan untuk menghitung rata-rata bandwidth 40 detik. Dari data-data tersebut diketahui bahwa:

$$\text{burst-limit} = 1024\text{kbps} (1\text{Mbps})$$

$$\text{longest-burst-time} = 10 \text{ detik}$$

$$\text{burst-time} = 40 \text{ detik}$$

Menghitung batas burst (*burst-threshold*) yang ideal untuk jaringan Anda dapat diketahui dengan rumus:

$$\text{burst-threshold} = (\text{burst-limit} * \text{longest-burst-time}) / \text{burst time}$$

$$\text{burst-threshold} = (1024 * 10) / 40 \text{ burst-threshold} =$$

$$(10240) / 40 \text{ burst-threshold} = 256\text{kbps}$$



Praktikum Management Jaringan

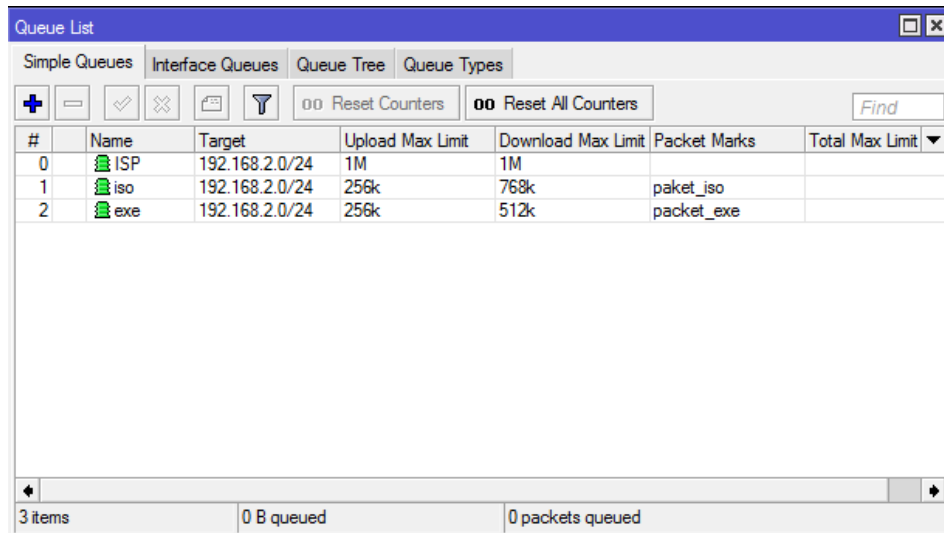
Setelah nilai *burst-threshold*, sekarang mari kita hitung berapa nilai ideal untuk *max-limit*:

$$\begin{aligned} \text{max-limit} &= 4/3 * (\text{burst-threshold}) \\ \text{max-limit} &= 4/3 * 256 \\ \text{max-limit} &= 342\text{kbps} \end{aligned}$$

Lalu kita lanjutkan menghitung nilai *limit-at* yang paling ideal. *limit-at* bisa dihitung dengan cara membagi nilai kecepatan maximal dengan jumlah client. Misalkan ada 7 komputer, maka

$$\begin{aligned} \text{limit-at} &= 1024/7 \\ \text{limit-at} &= 146\text{kbps} \end{aligned}$$

Sekarang kita masukkan nilai-nilai tersebut pada simple *Queue*. Jalankan Winbox, pilih menu *Queue* dan masuk ke tab *simple queue*.



#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit
0	ISP	192.168.2.0/24	1M	1M		
1	iso	192.168.2.0/24	256k	768k	paket_iso	
2	exe	192.168.2.0/24	256k	512k	paket_exe	

Gamabar 5.12 pemilihan queue yang akan di gunakan

Buat queue baru dengan nama burst, kemudian masukkan nilai – nilai yang sudah di hitung tadi

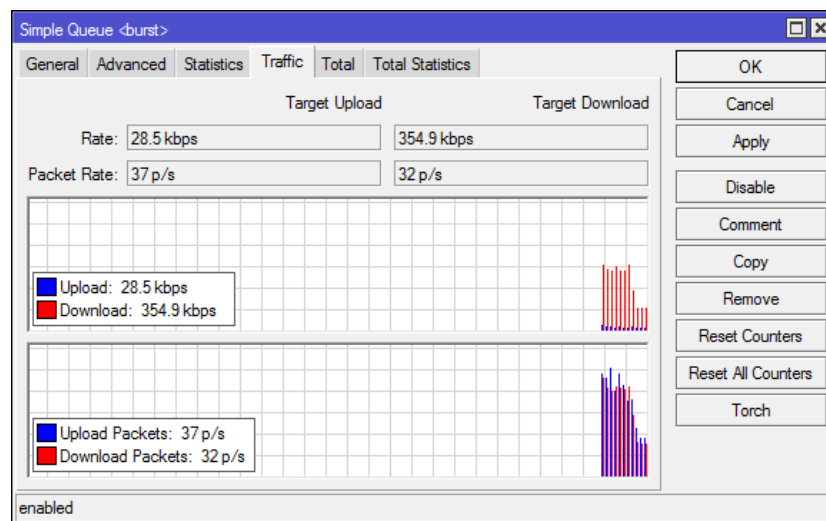


Praktikum Management Jaringan

The screenshot shows the 'Simple Queue <burst>' configuration window with the 'General' tab selected. The 'Name' field is set to 'burst' and the 'Target' is '192.168.2.0/24'. The 'Max Limit' for both Target Upload and Target Download is set to '342k'. The 'Burst' section shows a 'Burst Limit' of '1M' and a 'Burst Threshold' of '256k' for both directions. The 'Burst Time' is set to '40' seconds. The 'enabled' checkbox is checked. On the right, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters, and Torch.

Gambar 5.13 pengisian jumlah burst

Masukkan hasil perhitungan burst kedalam konfigurasi simple queue, kemudian klik apply, pindah ke tab advanced kemudian sesuaikan perhitungan pada limit at sesuai dengan perhitungan yang telah dibuat. Dan untuk hasil konfigurasi burst bisa di lihat pada gambar berikut :



Gambar 5.14 Tampilan Burst



Praktikum Management Jaringan

Dengan demikian kecepatan maximal pada saat *burst* diizinkan ada pada kisaran 2 Mbps. *Burst* diizinkan jika nilai rata-rata bandwidth (*average-rate*) kurang dari 256kbps yang dihitung dalam kurun waktu 40 detik. Jika lebih atau sama dengan 256kbps maka *burst* ditolak.

Kecepatan maksimal diperoleh hanya dalam waktu 10 detik, setelah itu bandwidth akan turun di kecepatan *max-limit* bahkan bisa 0 kbps. Mikrotik akan terus menghitung nilai *average-rate* dan membandingkannya dengan *burst-threshold*. Jika memenuhi syarat, bandwidth akan naik selama 10 detik dan turun setelah itu. Begitu seterusnya.



BAB VI HOTSPOT DAN MRTG

6.1 Hotspot

Hotspot merupakan area bersinyal yang berada pada tempat-tempat tertentu (biasanya tempat umum) yang memiliki layanan internet dengan menggunakan teknologi Wireless LAN, seperti pada perguruan tinggi, mal, plaza, perpustakaan, restoran, hotel ataupun bandara udara.

Fungsi Hotspot dalam jaringan wireless adalah sebagai pusat pemancar/penerima jaringan LAN (Local Area Network) yang kemudian Hotspot tersebut biasanya terhubung ke Internet. Sehingga laptop, notebook, atau smartphone yang berada pada area jangkauan Hotspot dan kemudian terhubung dengan jaringan hotspot itu maka biasanya akan bisa terhubung ke internet.

Ada beberapa jenis Hotspot yang biasa digunakan, yaitu:

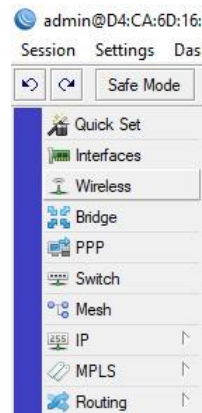
- Hotspot gratis sebagai tambahan pelanggan umum biasanya dioperasikan di hotel, di lobi hotel, di ruang konferensi, kedai kopi, atau di kafe. Kadang area bersinyal jenis ini merupakan instalasi semi permanen, di acara pameran komputer atau konferensi / seminar komputer.
- Hotspot yang dibayar langsung ke pemilik gedung, biasanya di ruangan hotel, restoran, atau kedai kopi. Tidak semua hotel mampu memberikan servis wi-fi gratis. Mereka mengambil kebijakan untuk memberikan servis berbayar kepada pengguna area bersinyal untuk mengganti biaya *leased line* atau tak terbatas (*unlimited*) ADSL ke Internet.
- Hotspot berbayar ke operator area bersinyal wi-fi, misalnya Boingo, iPASS. Operator area bersinyal wi-fi ini merupakan jaringan internasional yang global dengan banyak sekali pengguna yang berpindah tempat (*mobile*) secara internasional. Jenis area bersinyal ini biasanya akan lebih menarik bagi mereka yang memiliki banyak pengguna yang datang dari mancanegara.

Berikut adalah langkah-langkah Konfigurasi Hotspot :



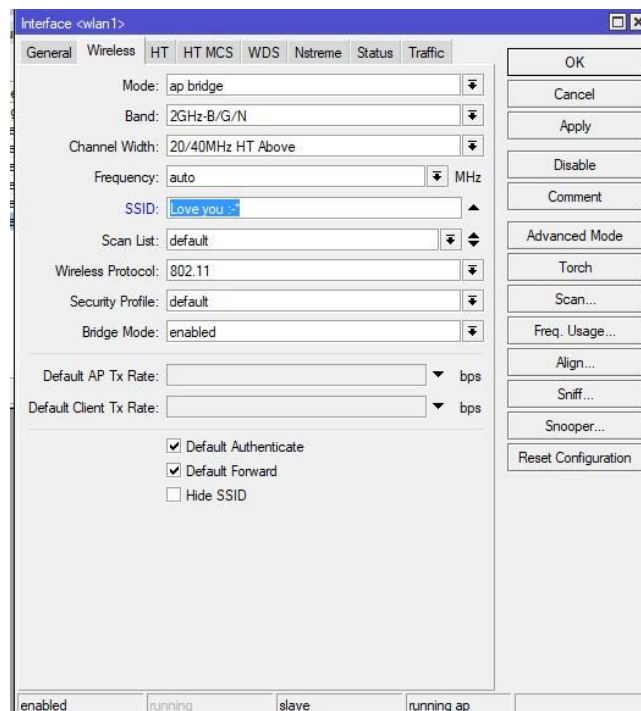
Praktikum Management Jaringan

1. Masuk pada winbox, dan pilih menu interface .



Gambar 6.1 Tampilan Interface

2. Pada menu interface pilih wlan1, pada tab wireless ganti mode menjadi ap Bridge dan isikan SSID yang digunakan sebagai identitas dari hostpost yang di setting seperti pada gambar berikut ini

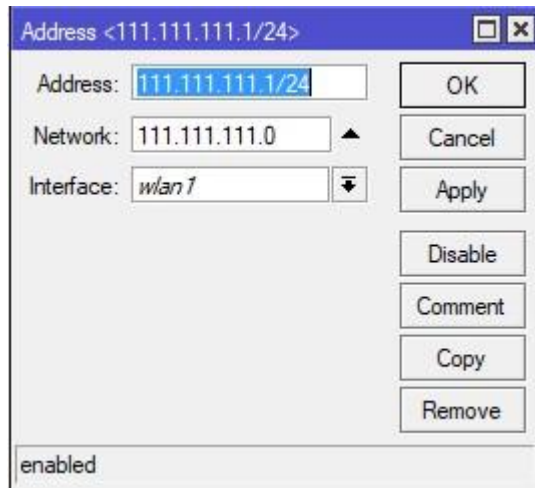


Gambar 6.2 Wireless Interface

3. Setting ip address yang akan digunakan untuk memberi alamat pada client, pilih ip > address dan setting ip seperti gambar berikut

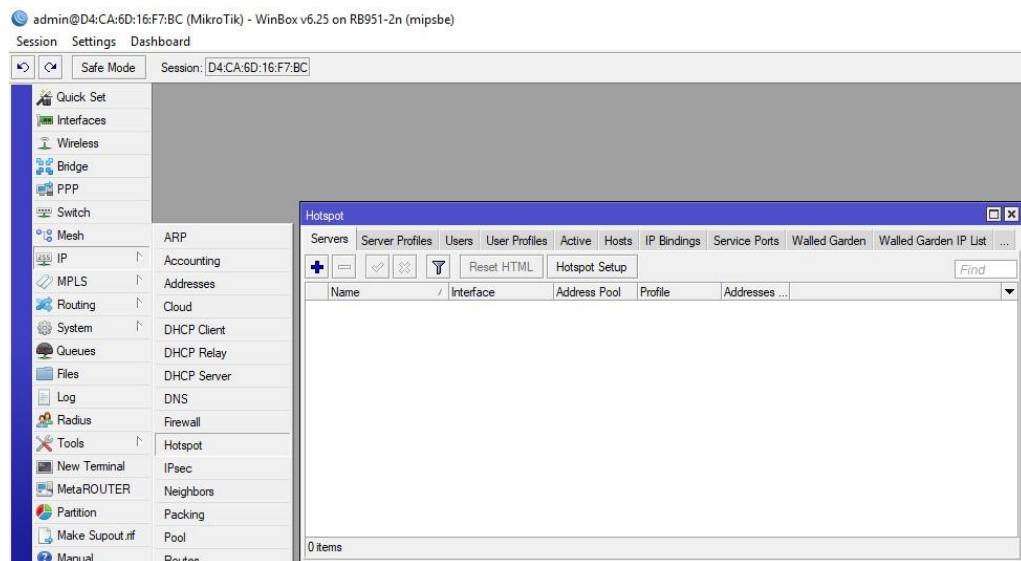


Praktikum Management Jaringan



Gambar 6.3 Setting IP Wireless

4. Setelah itu setting hotspot pada menu ip > hotspot untuk melakukan penyetingan hotspot dan pilih **hotspot setup** seperti pada gambar

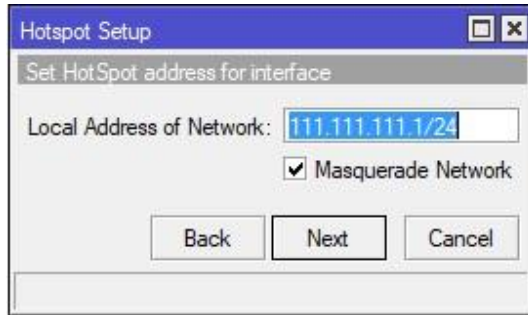


Gambar 6.4 Tampilan Hotspot

5. Selanjutnya mengisi IP address dari wlan1 dan centang Masquerade Network. klik Next

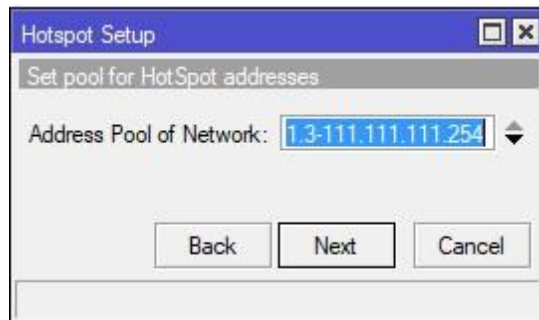


Praktikum Management Jaringan



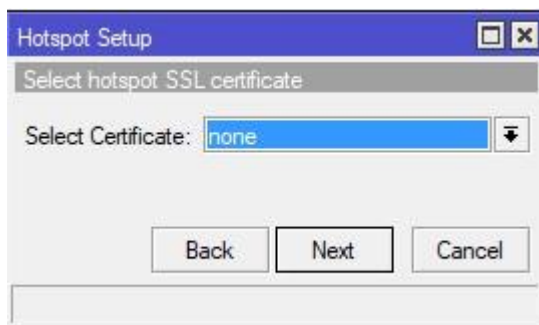
Gambar 6.5 Ip Address wlan1

- Menentukan range IP address yang akan diberikan ke user (DHCP Server),
misal : 111.111.111.3-111.111.111.254 Jadi user akan diberikan IP secara otomatis oleh DHCP Server antara range IP tersebut.



Gambar 6.6 Range IP

- Memilih SSL certificate. Pilih none saja, klik Next.

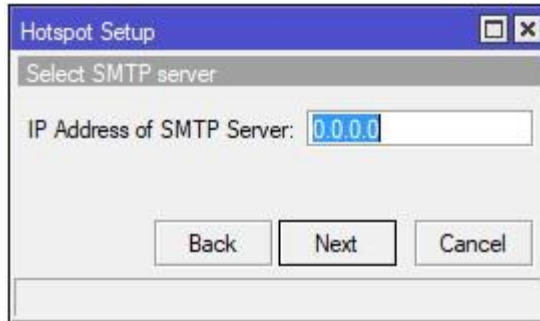


Gambar 6.7 SSL Certificate

- IP Address untuk SMTP Server kosongkan saja. Klik Next.

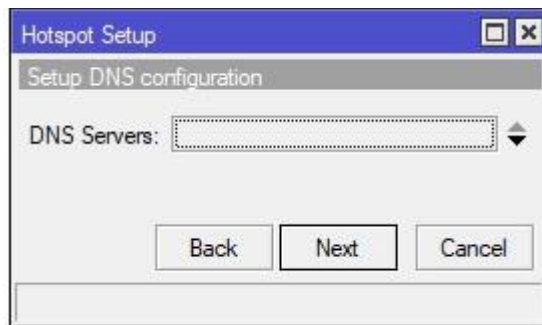


Praktikum Management Jaringan



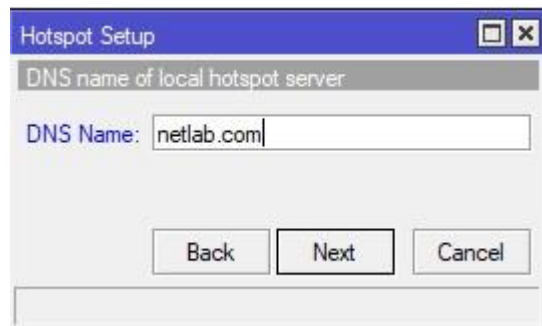
Gambar 6.8 SMTP Server

9. Memasukkan alamat DNS Server. Isikan saja dengan DNS Server nya Google : 8.8.8.8 dan 8.8.4.4. Klik Next.



Gambar 6.9 DNS Server

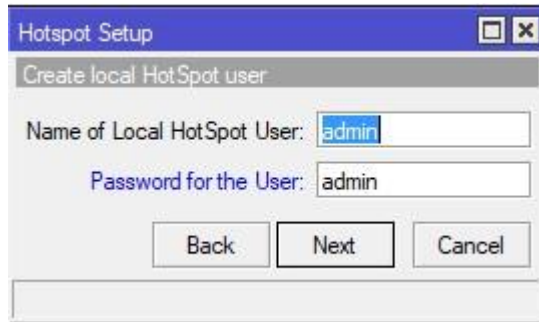
10. Memasukkan nama DNS untuk local hotspot server. Jika diisi nantinya akan menggantikan alamat IP dari wlan1 sebagai url halaman login. Jika tidak diisi maka url halaman login akan menggunakan IP address dari wlan1. Kosongkan saja, klik next.



Praktikum Management Jaringan

Gambar 6.10 DNS Name

11. Setting user pertama yang akan digunakan untuk login sebagai contoh username **admin** dan password **admin**.



Gambar 6.11 Hotspot Setup

12. Hotspot sudah berhasil dibuat dan silakan coba koneksikan laptop anda ke hotspot yang telah dibuat.



Gambar 6.12 Hasil Hotspot

13. Buka browser dan akses web, misalnya youtube.com maka anda akan dialihkan ke halaman login hotspot mikrotik.



Praktikum Management Jaringan



Gambar 6.13 Browser Youtube

6.2 MRTG

Berikut ini adalah tahap / langkah-langkah dalam membuat bandwidth Manajemen Mikrotik dan MRTG untuk monitoring bandwidth akses internet per-Client. Teknis setting bandwidth manajemen ini berlaku untuk semua jenis Mikrotik, baik Mikrotik Router

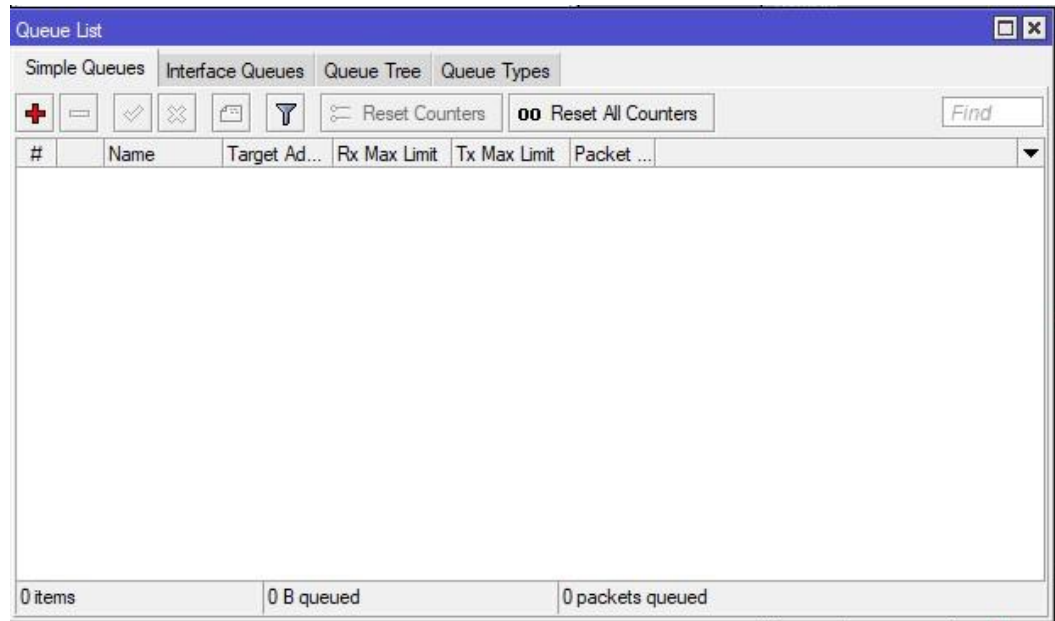


Praktikum Management Jaringan

Board, Mikrotik dengan Modem ADSL Mode PPPoE maupun Mikrotik dengan Modem ADSL Mode Bridge.

Berikut Langkah – langkah yang harus kita lakukan adalah :

1. Masuk menu Queues, seperti gambar dibawah ini :

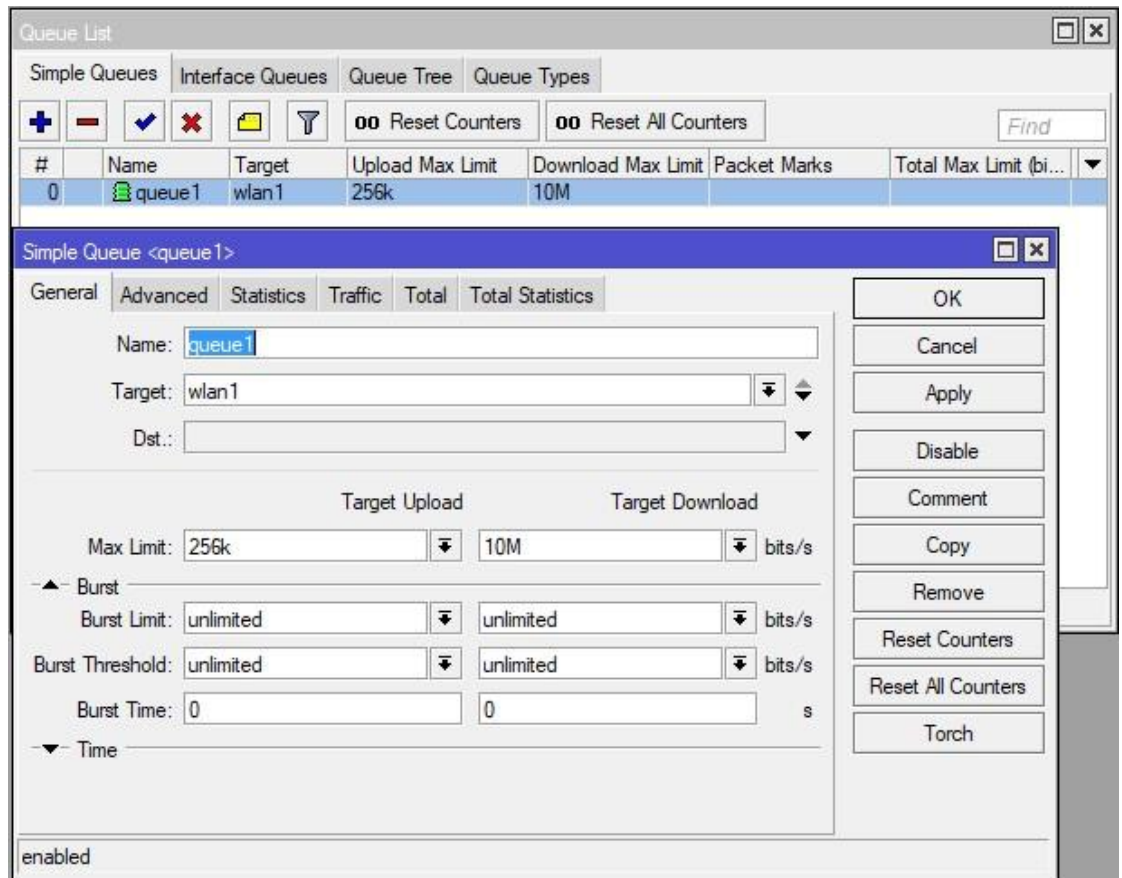


Gambar 6.14 Tampilan Menu Queues / Queue List

2. Pada menu tab general pilih tanda + kemudian akan muncul tampilan queue. berikan nama untuk queue nya kemudian pilih target ethernet yang akan dimonitoring. isikan max limit down dan up sesuai kebutuhan. Kemudian klik ok.



Praktikum Management Jaringan

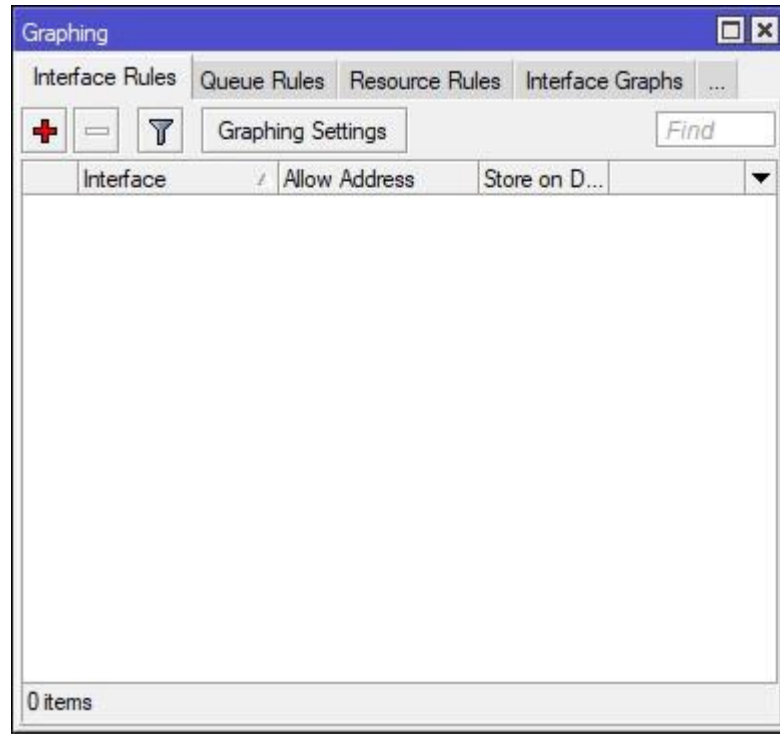


Gambar 6.15 Tampilan tab General

- Setelah melakukan konfigurasi pembuatan user client, langkah selanjutnya yang akan dibuat adalah membuat MRTG dari Simple Queue yang telah kita buat tadi. Masuklah ke menu Tools lalu pilih Graphing seperti pada gambar 6.16.



Praktikum Management Jaringan

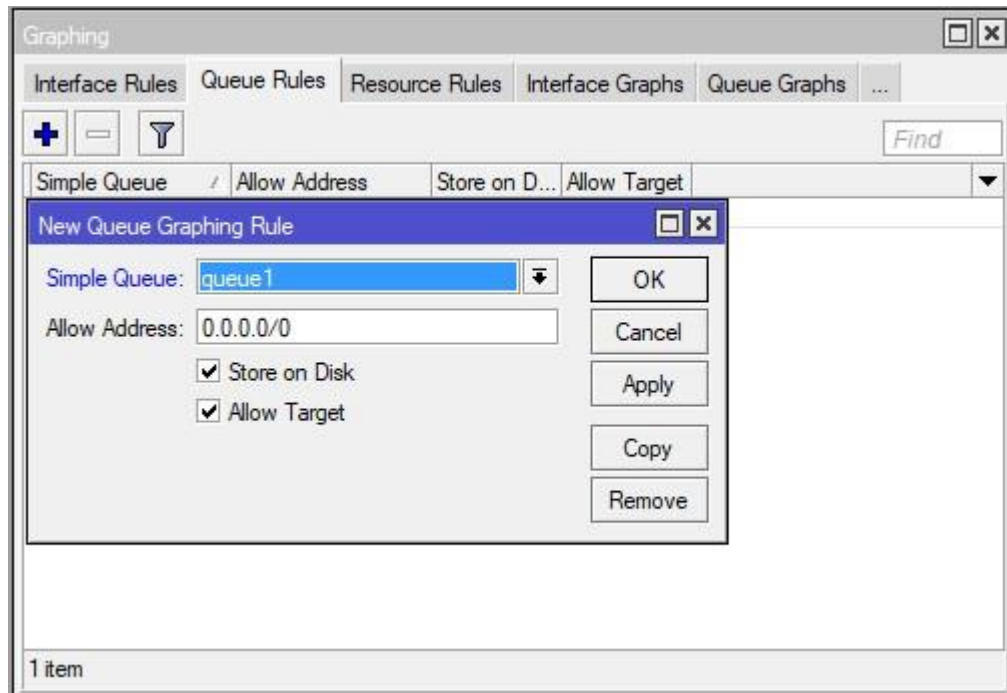


Gambar 6.16 Tampilan Graphing

4. Selanjutnya Kita pilih menu Queue Rules, lalu pada option Simple Queue kita pilih nama Queue yang telah kita buat melalui menu Drop Down seperti pada gambar 6.17



Praktikum Management Jaringan

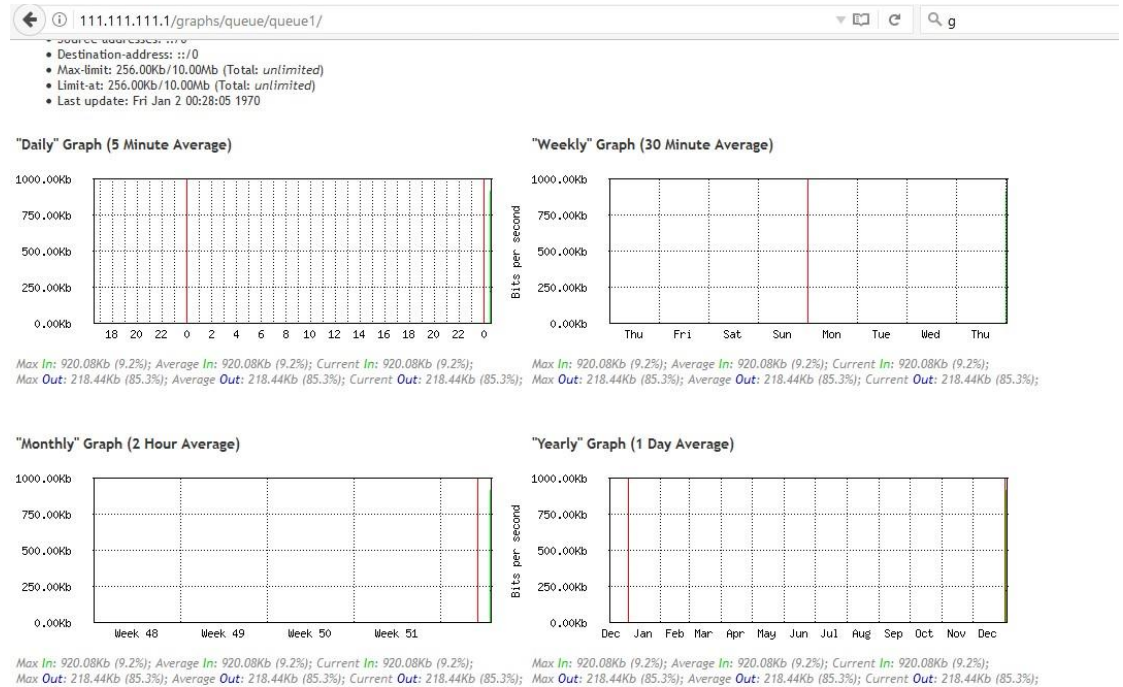


Gambar 6.17 Tampilan Queue Rules

5. Pada saat membuka Webfix pastikan ip anda dalam satu jaringan dengan ip dari gateway mikrotik agar dapat terhubung langkah selanjutnya adalah menampilkan interface static dengan cara menghubungkan yang sama, namun ada penambahan setelah <http://111.111.111.1/graphs/> pada ip dan pilih nama graph yang udah kita buat tadi adapun langkahnya seperti pada gambar 6.18



Praktikum Management Jaringan

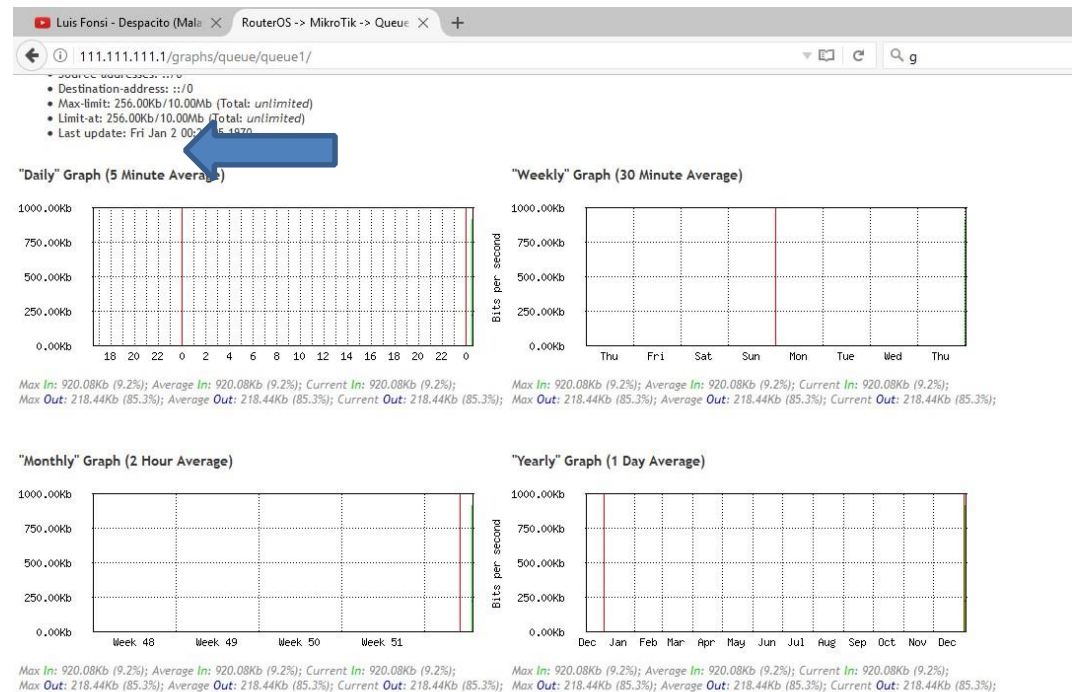


Ganbar 6.18 Tampilan



Praktikum Management Jaringan

6. Pada langkah yang selanjutnya maka yang anda lakukan adalah membuka tampilan dari queue statics yang akan menampilkan source address, destination address dan max limit yang hasilnya akan seperti pada gambar 6.19.



Gambar 6.19 Tampilan



Selamat Mengerjakan Laporan Praktikum

