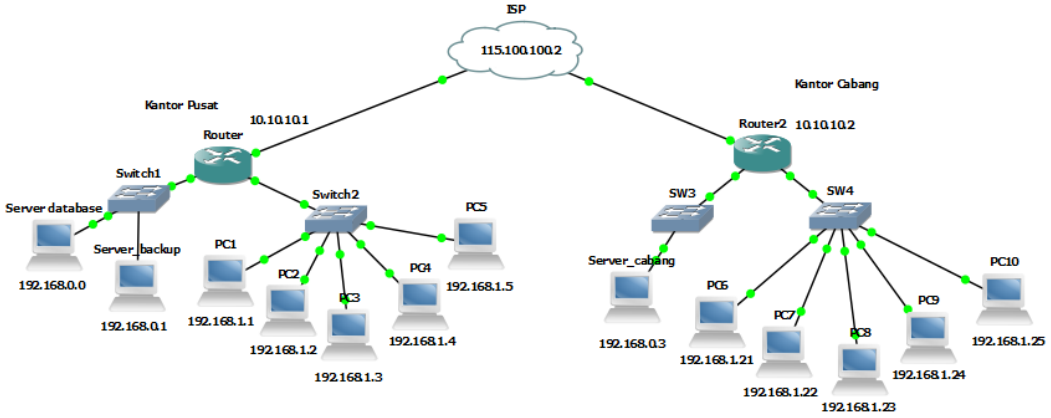
BAB lV

RANCANGAN JARINGAN

4.1 Jaringan Usulan

Pada bab ini penulis ingin mengajukan jaringan usulan dari apa yangpenulis telah analisa sebelumnya setelah riset pada PT. Dharma Putra Sentosa. Didalam skripsi ini penulis ingin memberikan jaringan usulan agar kantor cabangdan pusat dapat saling berkomunikasi layaknya seperti dalam satu



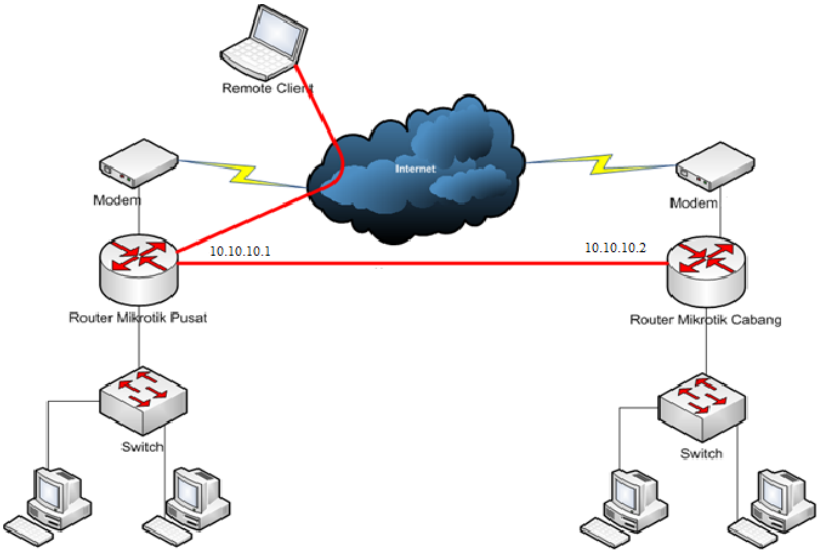
jaringan.

Sumber : Penulis

Gambar IV.1 Jaringan Usulan PT. Dharma Putra Sentosa

4.1.1 Topologi Jaringan

Dalam mengusulkan topologi jaringan yang akan diimplementasikan pada PT. Dharma Putra Sentosa, penulis tidak akan merubah bentuk topologi yang sudah ada, hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan kantor pusat dan cabang menggunakan topologi *star*. Penulis mengusulkan untuk menggunakan mikrotik untuk memenejement bandwith antar kantor pusat menjadi lebih aman.



Sumber : Penulis

Gambar IV.2 Topologi Jaringan PT. Dharma Putra Sentosa

4.1.2 Skema Jaringan

Pada rancangan jaringan usulan ini, di sisi router kantor pusat yang sudah terkonfigurasi ip publik untuk akses internet 118.98.222.2 dan ip private 192.168.1.0 sebagai *gateway* MAN, dan ip route10.10.10.1/30 pada router Mikrotik. Kemudian di sisi cabang yang sudah terkonfigurasi ip private 192.168.2.0 sebgai *gateway* MAN, serta mengatur konfig management menggunakan mikrotik router sebagai jalur akses.

4.1.3 Keamanan Jaringan

Untuk Keamanan jaringan yang digunakan pada implementasi kali ini kamimenggunakan fitur kemanan dengan menggunakan mikrotik router, Firewall yang terdapat dalam mikrotik router untuk mengatur pembagian bandwith dan ip pemblokiran . Dan kami jugamenerapkan *filter rule* pada *firewall* di mikrotik untuk membatasi akses ke serverhanya dari ip *address* tertentu. Dalam juga penulis membedakan jaringan pada kantor pusat dan kantor cabang. Dari sisi

kantor pusat, penulis menggunakan Net ID 192.168.0.0/24 dan pada kantor cabang menggunakan Net ID 172.16.10.0/24. Selain itu juga tidak memberlakukan *mode bridge* dikarenakan Net ID Pusat dan Cabang yang berbeda serta menjauhi adanya *broadcast* virus dari cabang ke kantor pusat ataupun sebaliknya. Untuk itu routing dibuat terpisah, yaitu routing ke arah internet dan routing ke arah jaringan MANkantor.

4.1.4 Rancangan Aplikasi

Untuk menggunakan jaringan MAN dengan menggunakan Mikrotik Router maka harus dilakukan konfigurasi pada router kantor pusat dan router cabang PT. Dharma Sentosa. Tahapannya adalah sebagai berikut :

4.1.5 Manajemen Jaringan

Setelah penulis menganalisa system jaringan berjalan pada PT. Dharma Putra Sentosa, maka penulis mengusulkan sebuah jaringan menggunakan firewall untuk kemanan yang mengatur pembagian bandwidth dan pemblokiran ip address bagi client yang terdapat di perusahaan tersebut.

Dengan menggunakan router mikrotik, kemudian dikonfigurasi untuk menerapkan system jaringan man baik kantor pusat dan kantor cabang.

4.2. Pengujian Jaringan

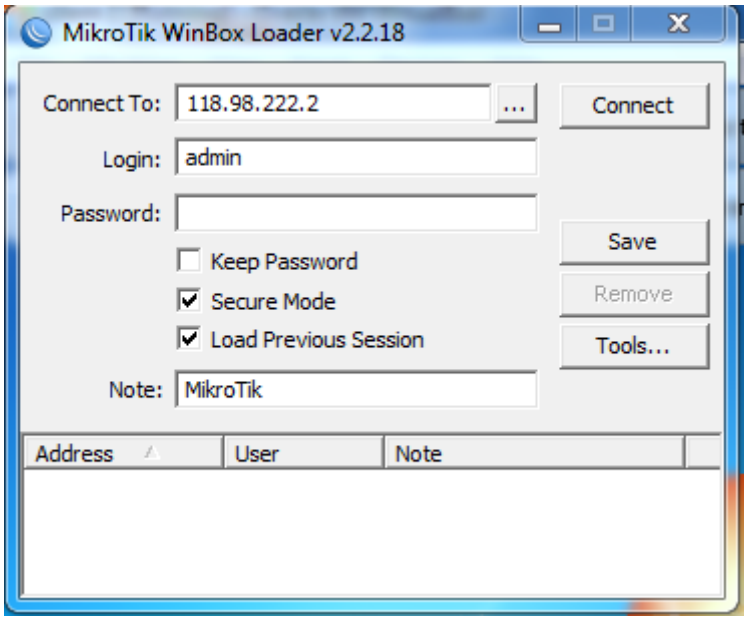
Pengujian jaringan dilakukan di awal sebelum masuk winbox dibuat, dan mengatur firewall yang terkonfigurasi, hasil akhir pengujian yang dilakukan adalah dengan melakukan pengaturan pada system mikrotik router yang dimana nanti akan dijelaskan pada bagian selanjutnya, untuk mengatur jaringan kantor pusat dan kantor cabang.

4.2.1. Pengujian Jaringan Awal

Konfigurasi pengujian awal mikrotik router harus terakses dengan internet dengan pengujian yang mengatur DHCP, DNS dan MAC ADDRESS yang sudah diaktifkan pada mikrotik, pengujian dilakukan dengan test ping ke mikrotik serta memblokir ip address yang sudah terdapat di DHCP mikrotik.

1 Winbox

Sebelum masuk dan melakukan konfigurasi ke sistem, terlebih dahulu digunakan aplikasi *WinBox* untuk me-r*emote router*. Dalam penggunaan aplikasi *WinBox* dibutuhkan alamat IP *router*, IP user beserta *password* dari *router* yang akan di *remote*.



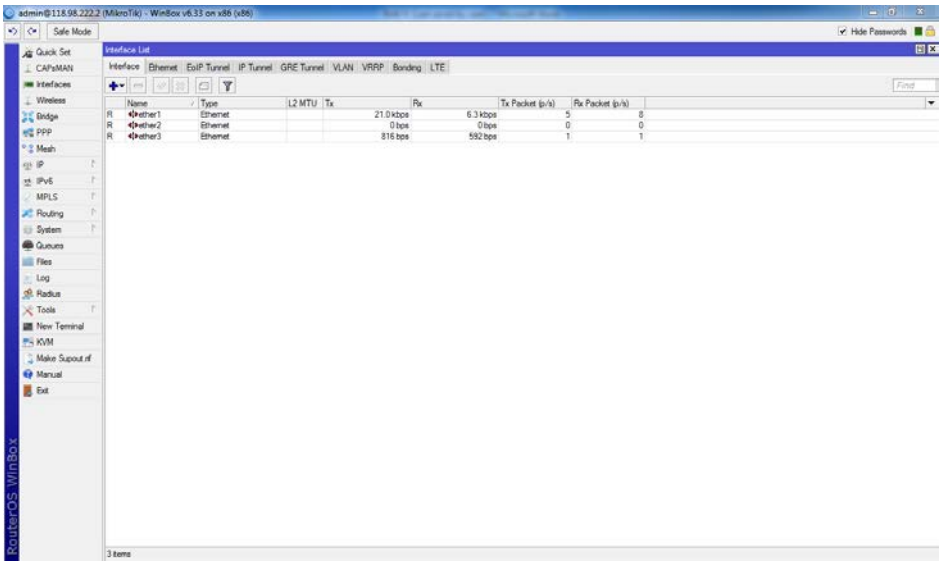
Sumber : Penulis

Gambar IV.3. Aplikasi winbox

2 Interface

Tabel *interface* berfungsi sebagai tabel pemantau jumlah *Lancard* yang terdeteksi oleh perangkat *router*. Didalam *table interface* ini juga dapat melakukan pelabelan terhadap *Lancard* yang telah dikenali

sebelumnya supaya tidak terjadi kesalahan peletakan IP *address* ataupun pemasangan kabel jaringan. Didalam table *interface* ini juga dapat terpantau apakah kabel jaringan sudah terkoneksi ataupun belum terkoneksi.



Sumber : Penulis

Gambar IV.4. Interface

3. Implementasi *Limiter Queue Tree*

Di dalam tabel *queue* list terdapat beberapa tipe limiter antara lain*simple queue* dan *queue tree*. Di dalam tab *queue tree* terdapat fungsi menambahkan *limiter*, menghapus *limiter*, mematikan *limiter* dan mengaktifkan *limiter*.Ke empat fungsi diatas adalah fungsi-fungsi yang sering digunakan dalam implementasi *system limiter*. Apabila fungsi yang dipilih adalah fungsi *ADD* atau menambahkan yang di wakili dengan tanda (+) berwarna merah, maka akan tampil kotak dialog yang berisi keterangan-keterangan untuk diisi.

1. *Name* : dalam kolom *name* dapat diisikan dengan nama perangkat yang akan di *limit*.

2. *Parent* : dalam kolom *parent* berfungsi untuk menentukan *limiter* tersebut menginduk ke *limiter* lain atau ke salah satu *interface*

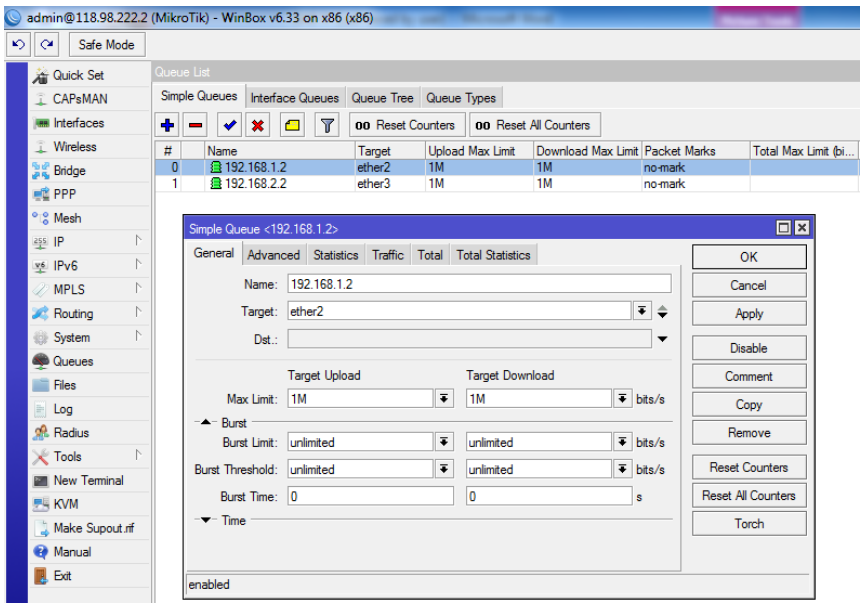
3. *Packet Marks* : dalam kolom *packet marks* di tentukan paket koneksi yang akan di *limit*

4. *Queue type* : dalam kolom *queue type* dapat dipilih jenis *limiter* yang telah dibuat sebelumnya didalam tab *Queue Types*

5. *Priority* : dalam kolom *priority* berfungsi untuk menentukan prioritas urutan *limiter* yang akan dijalankan terlebih dahulu.

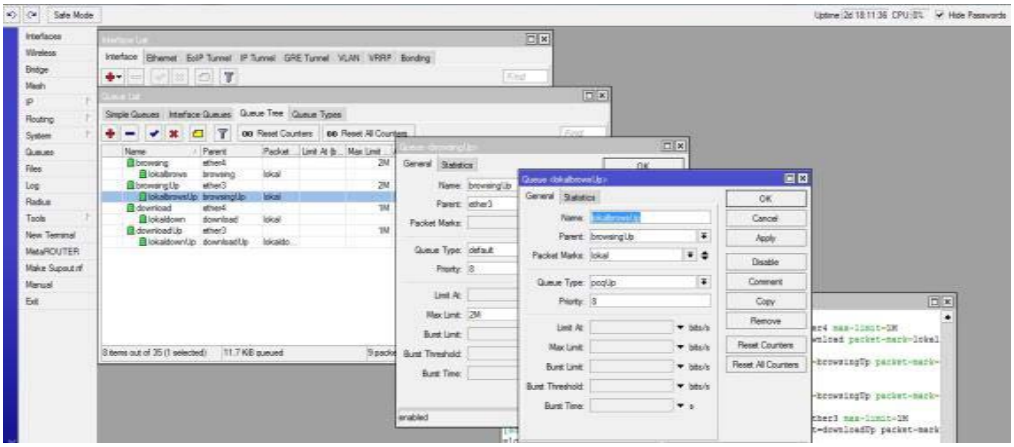
6. *Limit at* : di dalam kolom max limit terdapat besaran bandwith yang berfungsi sebagai pembatas minimal.

7. *Max Limit* : di dalam kolom max limit terdapat besaran bandwith yang berfungsi sebagai pembatas maksimal.



Sumber : Penulis

Gambar IV.5. Kotak dialog *queue tree limit download*

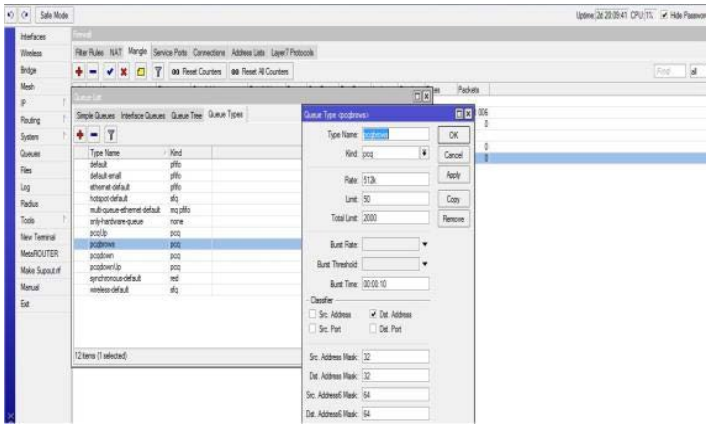


Sumber : Penulis

Gambar IV.6. Kotak dialog *queue tree limit upstream*

4. Implementasi Queue Types

Queue type berfungsi untuk membantu mengatur kerja *limiter* baik pada *simple queue* maupun *queue tree*. Dengan menggunakan *queue type* dapat memudahkan dalam pembatasan kecepatan tanpa harus memasukkan besaran *limiter* pada masing-masing IP yang akan dibatasi kecepatannya.



Sumber : Penulis

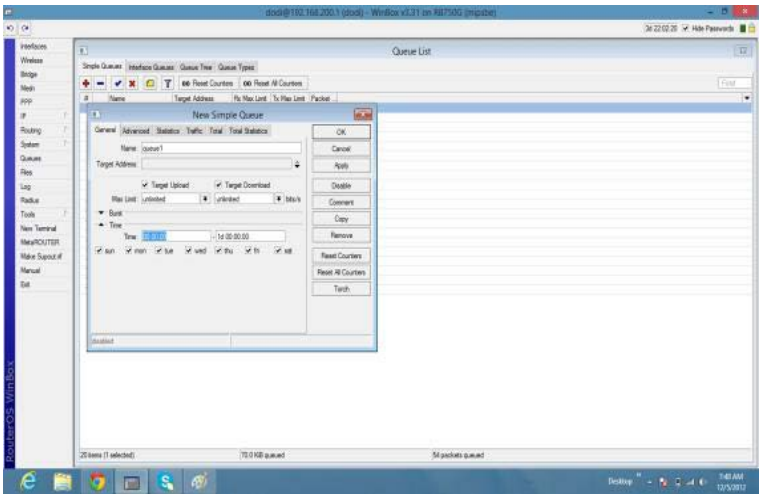
Gambar IV.7. Kotak dialog *queue type*

Pada gambar diatas terdapat beberapa kolom yang memiliki *value*.Pada kolom-kolom diatas yang harus diubah *value* adalah kolom *Type Name* yang akan

menjadi nama untuk *queue type* yang dibuat dan pada kolom *Rate* yang akan berfungsi sebagai pembatasan kecepatan maksimal pada masing-masing IP..

5. Implementasi *Timer* pada *Simple Queue*

Di dalam *limiter simple queue* terdapat juga fitur *time*. Fitur *time* biasanya difungsikan apabila terdapat dua sistem atau lebih besaran konfigurasi *limiter* yang akan digunakan. Misal dalam implementasi terdapat dua konfigurasi besaran limiter antara waktu siang dan malam, fitur *time* dapat diaktifkan supaya tidak perlu mematikan dan menghidupkan limiter secara manual cukup mengaktifkan fitur *time*, maka limiter akan berganti secara otomatis



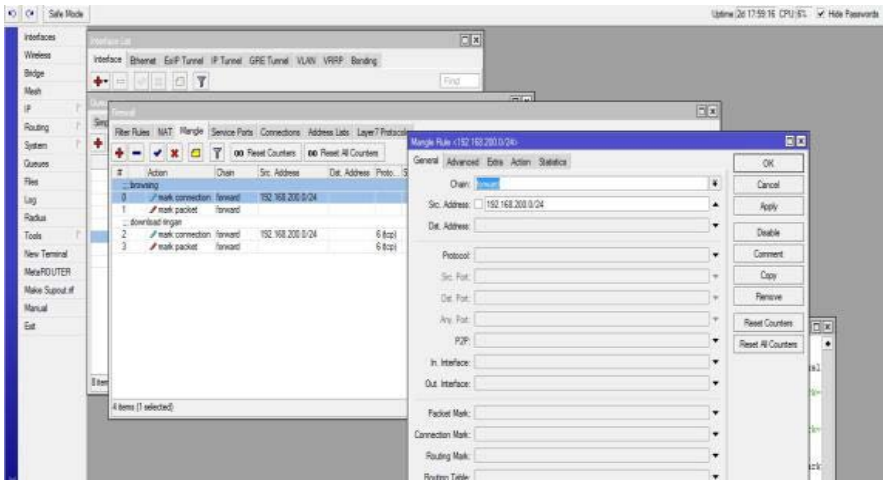
Sumber : Penulis

Gambar IV.8. Fitur *time* pada *simple queue*

6. Implementasi Mangle

Untuk dapat mengaktifkan pembatasan *bandwith* di *queue tree*, sebelumnya perlu menambahkan *mangle* pada *firewall mangle* yang berfungsi untuk menandai paket koneksi yang berasal dari klien. Dalam konfigurasi *queue tree* diatas, pembatasan *bandwith* di bagi menjadi dua yaitu *limiter download* dan *limiter browsing*. Dengan pemisahan *limiter* seperti diatas maka pada konfigurasi

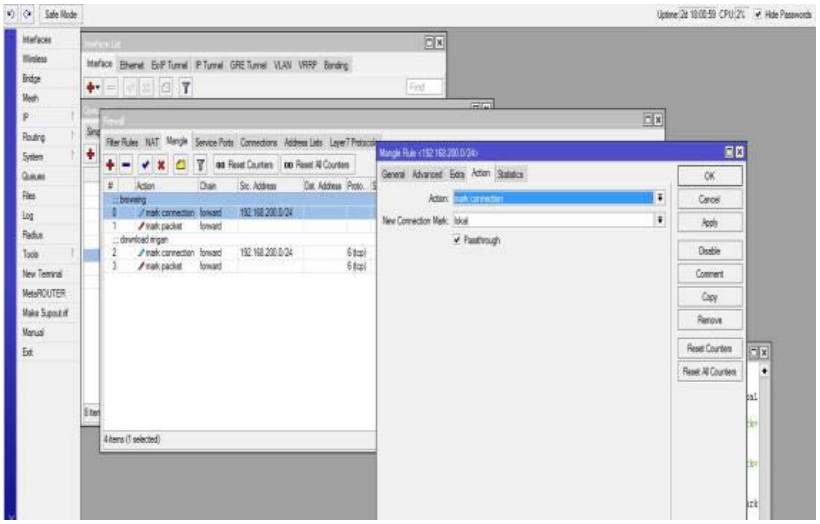
mangle memerlukan dua konfigurasi untuk dapat menjalankan konfigurasi *limiter* tersebut



.

Sumber : Penulis

Gambar IV.9. Konfigurasi *mangle browsing*

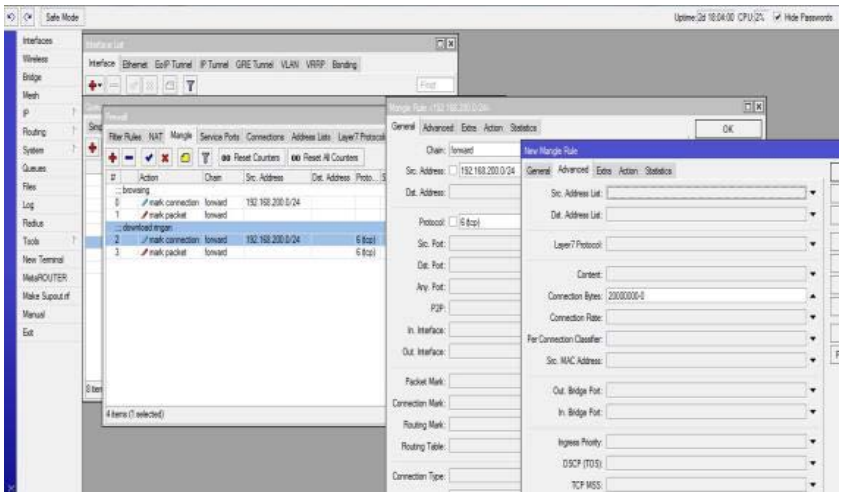


Sumber : Penulis

Gambar IV.10. Konfigurasi mangle browsing 2

Pada gambar pertama terlihat pada kolom Src. Address terdapat IP 192.168.200.0/24 yang merupakan IP dari *network* lokal, kemudian di gambar

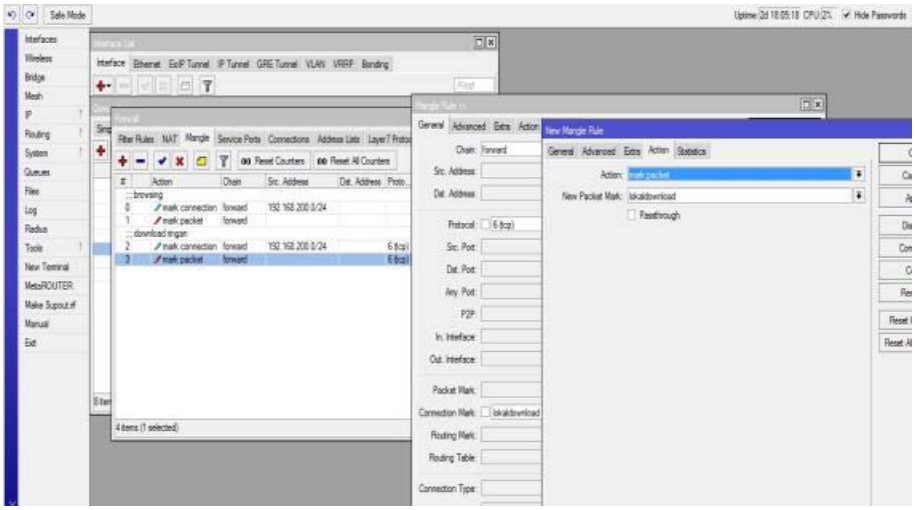
kedua *network* IP tersebut dilabeli dengan nama “lokal”. Paket dengan nama “lokal” tersebut yang akan di jadikan parameter *limiter* di *queue tree* paket browsing.



Sumber : Penulis

Gambar IV.11. Konfigurasi mangle download

Dalam gambar diatas terlihat Src. Address yang sama dengan *mangle browsing*, hal ini dikarenakan IP tersebut merupakan IP dari *network* lokal pada jaringan diatas. Yang menjadi perbedaan adalah pada bagian Connection Bytes pada gambar diatas terdapat parameter angka 20000000-0, yang berarti konfigurasi *mangle* diatas akan menangkap paket apabila klien telah melakukan *request* paket hingga 20MB



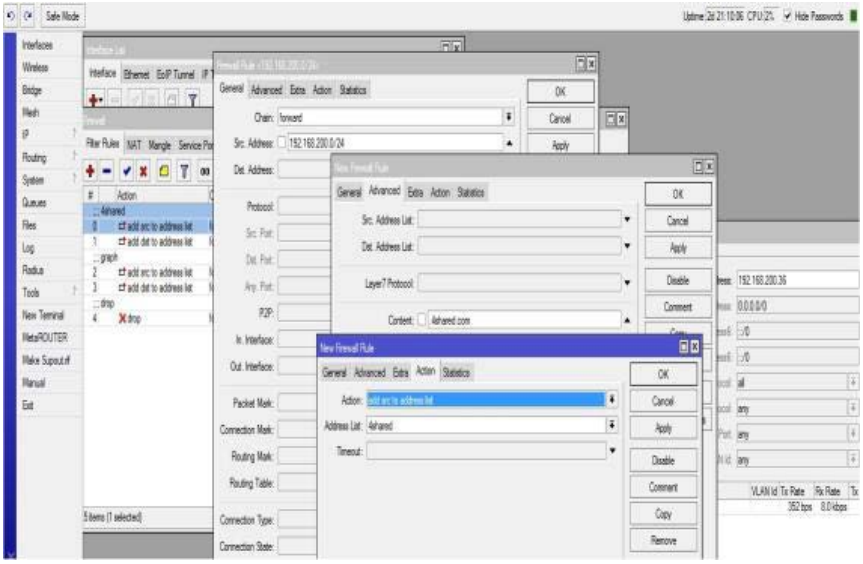
Sumber : Penulis

Gambar IV.12. Konfigurasi *Mangle Download* 2

Pada gambar diatas paket yang telah ditandai dengan parameter Connection Bytes kemudian dilabeli dengan nama “lokaldownload” yang nantinya akan digunakan sebagai parameter *limiter download* pada konfigurasi *queue tree*.

7. Implementasi Firewall Filter Rules

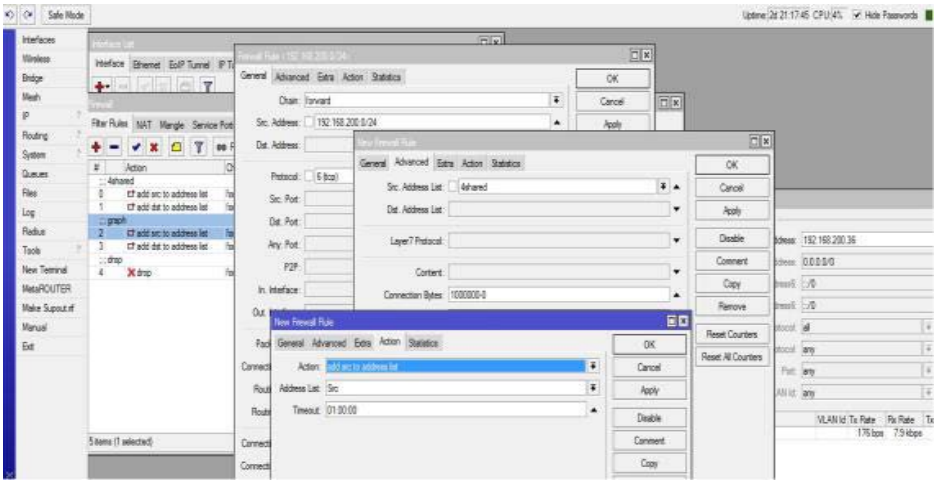
Selain proses pembatasan kecepatan *browsing* maupun *download* yang di *handle* oleh *queue tree* dan *mangle*, dapat juga dilakukan penutupan akses *download* atau *browsing* ke alamat *website* tertentu. Untuk melakukan hal tersebut dapat menggunakan *filter rules* yang dikombinasikan dengan *address list* sebagai penyimpanan IPnya.



Sumber : Penulis

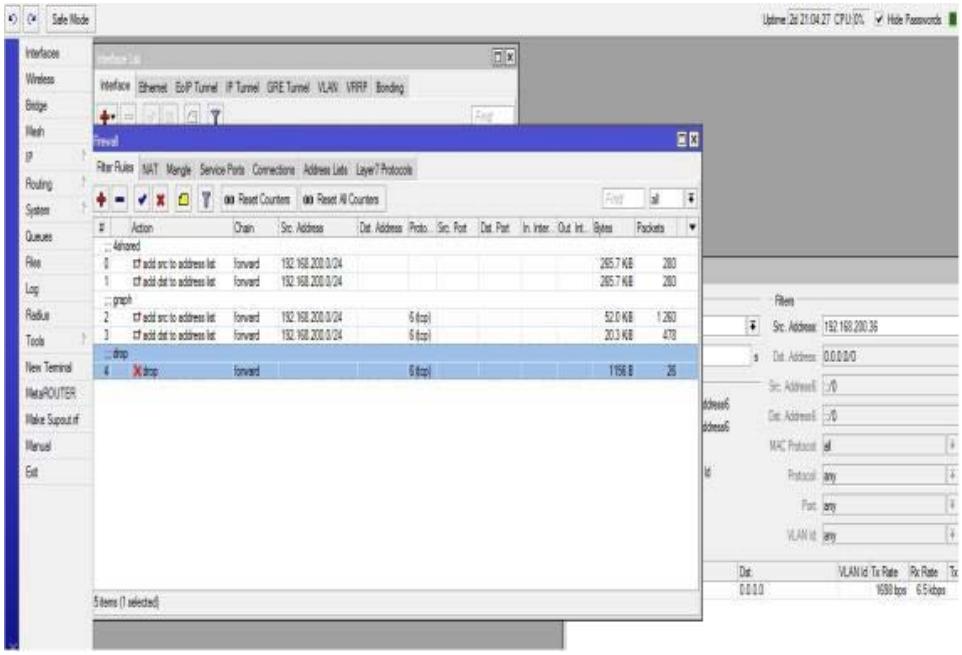
Gambar IV.13. Konfigurasi filter rules tandai IP website

Pada gambar diatas konfigurasi filter rules berfungsi untuk menangkap IP dari website yang akan difungsikan sebagai parameter DROP. Setelah IP dari website yang akan dijadikan paremeter tersimpan di address list scrip koonfigurasi selanjutnya bertugas sebagai parameter besaran request paket yang di ambil oleh klien menggunakan fitur connection byte kemudian IP tersebut akan disimpan kembali di address list dengan nama Src dan Dst. Dan setelah IP klien selesai ditandai dan tersimpan di dalam address list, maka konfigurasi terakhir berfungsi sebagai penutup jalur koneksi yang menuju alamat website tersebut dengan besaran request paket yang telah tercapai sesuai pada parameter dari script konfigurasi kedua.



Sumber : Penulis

Gambar IV.14. Konfigurasi filter rules tandai IP klien

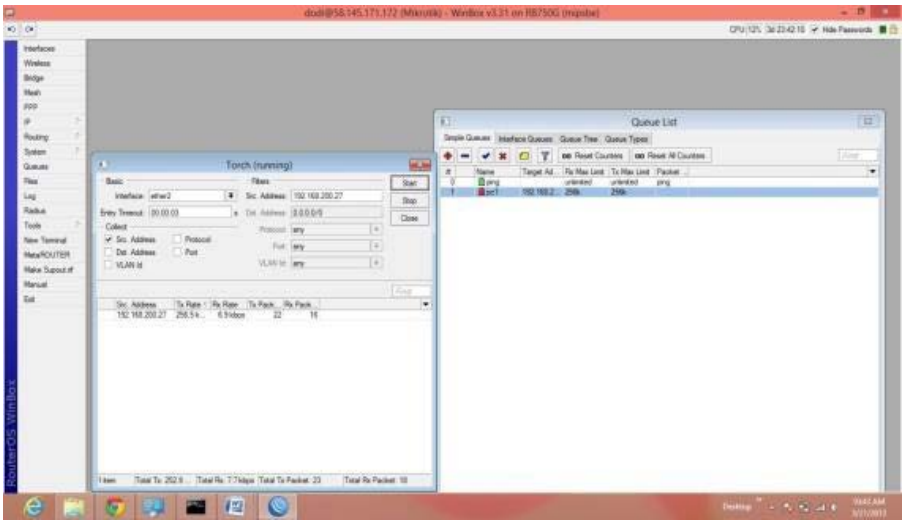


Sumber : Penulis

Gambar IV.15. Konfigurasi filter rules DROP koneksi

8. Pengecekan Limiter Melalui Torch

Setelah proses konfigurasi *limiter* selesai maka proses selanjutnya adalah pengecekan berfungsi atau tidaknya *limiter* tersebut. Sebagai contoh pc1 dengan Ip *address* 192.168.200.27 dilimit dengan *max-limit* sebesar 256kbps. Pada gambar terlihat bahwa Pc1 telah mencapai kecepatan maksimal yang di berikan (terlihat dari warna merah pada symbol Pc1). Kemudian di tabel torch di samping kiri terlihat bahwa ip 192.168.200.27 telah mencapai kecepatan 256kbps. Dengan hasil tersebut maka limiter telah berhasil di implementasikan pada router ini.

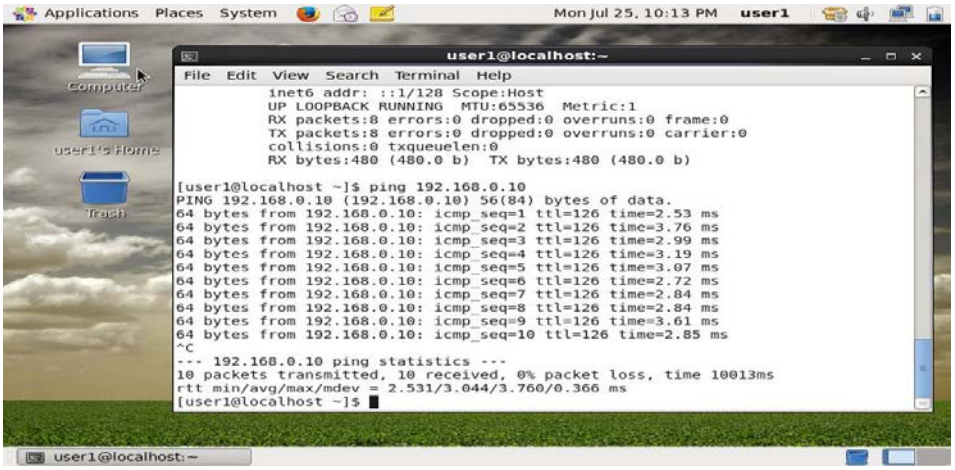


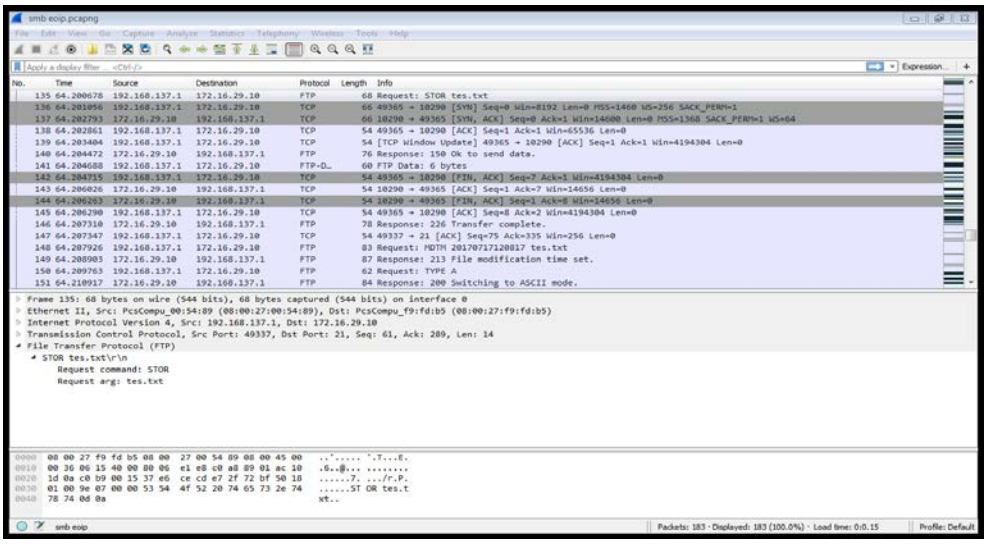
Sumber : Penulis

Gambar IV.16. Pengecekan limiter

4.2.2 Pengujian Jaringan Akhir

Pada hasil akhir pengujian jaringan ini dilakukan berdasarkan tes ping dan ping jaringan ke arah kantor pusat dan cabang untuk mengetahui bahwa jalur yang dikirim baik dari sisi pusat ke cabang atau sebaliknya adalah jalur melalui *gateway* yang sudah dikonfigurasi sebelumnya.





Sumber : Penulis

Gambar IV.17. Pengujian dengan wireshark

Setelah terjadinya koneksi intranet yang ada di kantor pusat dan kantor cabang , maka kita dapat berbagi akses dan kemudahan untuk membentuk satu jaringan berskala *Metropolitan Area Network* (MAN) sehingga seluruh staff dapat memanfaatkan *resource* seluruh jaringan yang ada untuk terhubung ke jaringan MAN yang ada di kantor pusat dan cabang tanpa harus membuat suatu autentifikasi user terlebih dahulu. Karna mikrotik sudah melakukan penyetingan mikrotik dan user yang tidak terdapat dikonfik tidak akan bias masuk ke dalam jaringan pada divisi terkait.