BAB IV

IMPLEMENTASI DAN PENGUJIAN

4.1 IMPLEMENTASI

Gambaran umum tahap implementasi yang harus dilakukan sebagai berikut :

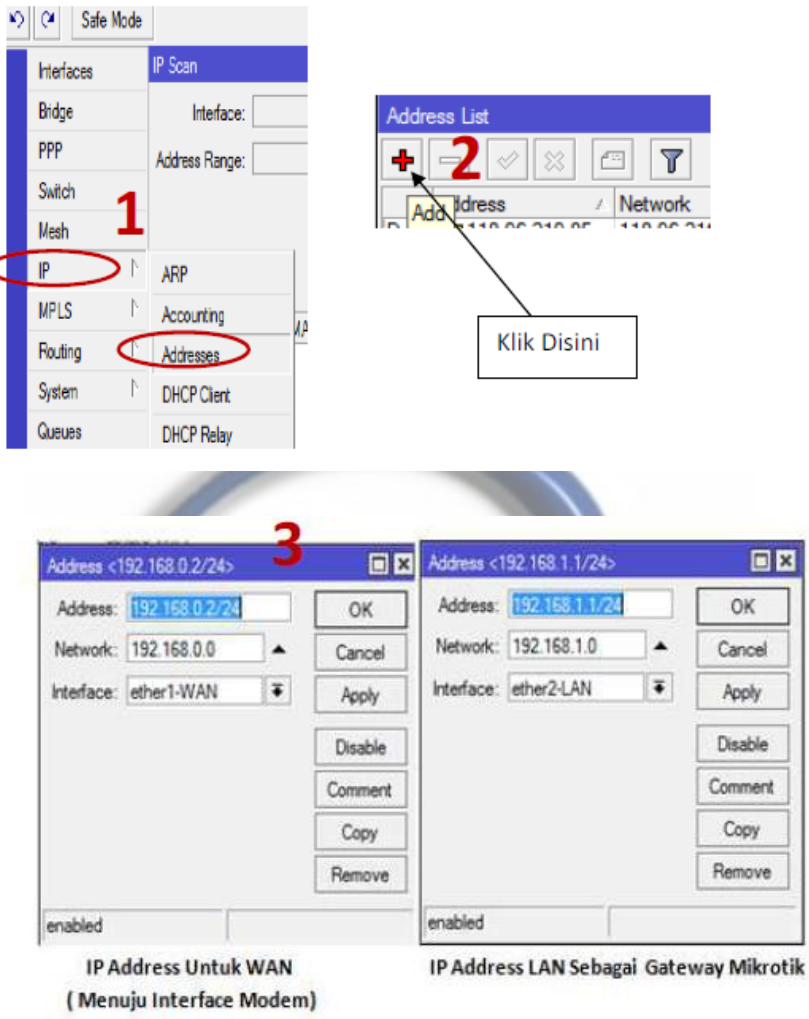
1. Proses konfigurasi pengalamatan IP *Address*
2. Proses konfigurasi *management bandwidth*
3. Proses konfigurasi Radius *Server*
4. Proses konfigurasi blokir Web di mikrotik
5. Proses konfigurasi pengamanan mikrotik dari serangan

4.1.1 Proses Konfigurasi Pengalamatan IP *Address*

Disini penulis untuk awal melakukan konfigurasi alamat IP *Address* sesuai dengan *disegn* perancangan jaringan yang telah di buat oleh penulis. Untuk pengalamatan IP *Address* sebagai berikut :

1. Ether 2 192.168.1.1/24 DHCP
2. Ether 3 192.168.9.1/24 *Static*
3. Ether 4 192.168.10.1/24 DHCP

Caranya Masuk ke menu IP dan Pilih *Address* kemudian tambahkan IP ddress dengan mengklik Icon Plus + akan muncul tampilan New *Address* kemudian anda isikan seperti berikut



Gambar 4.1 Pengalamatan IP Address

1. Via Terminal

Set Ip *Address* :

/ip *Address* add *Address* 192.168.1.1/24 interface=ether2-LAN

/ip *Address* add *Address* 192.168.1.1/24 interface=ether2-LAN

/ip *Address* add *Address* 192.168.1.1/24 interface=ether2-LAN

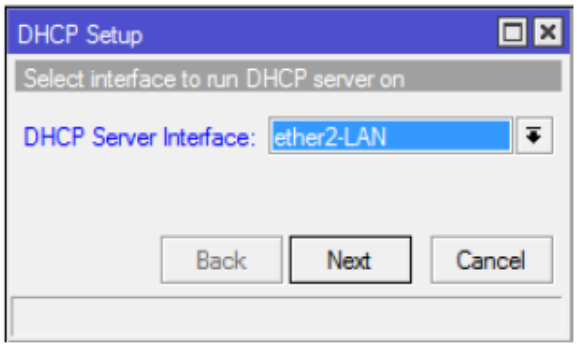
2. Setting DHCP *Server*

DHCP *Server* (Dynamic Host Configuration Protocol) adalah Sebuah *Server* yang menyediakan Services atau memberikan layanan IP *Address* Otomatis bagi *Client* yang IP *Address* -nya di setting Automatic. DHCP *Server* menyediakan konfigurasi IP *Address* Otomatis yang meliputi : IP *Address* , IP *Gateway* dan IP DNS *Server* . Untuk bisa *Client* laptop mengakses jaringan wifi dengan cara menggunakan ip Dynamic adalah harus set DHCP *Server* di mikrotik. Langkahnya adalah sebagai berikut:

1. Klik IP – DHCP *Server*

Gambar 4.2 Konfigurasi DHCP Server

2. Selanjutnya Klik DHCP Setup,



Gambar 4.3 Pemberian IP Pada Ether

3. Pada Gambar 4.2 diatas tentukan *Server* Interfacenya Pilih ether-2 LAN.
4. Selanjutnya Pada Gambar diatas menentukan DHCP *Address Space*. Karena IP *Address* jaringan LAN adalah 192.168.1.xxx/24 maka secara otomatis Wizard akan menawarkan DHCP *Address Space* : 192.168.1.0/24
5. Selanjutnya menentukan IP *Gateway* untuk DHCP ini. IP *Gateway* adalah IP *Address* dari interface yang menjembatani antara jaringan LAN dan Mikrotik, tentunya pada contoh kasus ini menggunakan IP *Address* : 192.168.1.1, lalu klik *Next*.
6. Selanjutnya menentukan DHCP IP *Address Range* alias alokasi IP *Address* yang akan di layani untuk *Client*.
7. Selanjutnya menentukan IP *Address* DNS *Server* . Disini dapat mengunakan IP DNS yang di gunakan oleh *Provider* atau bisa mengunakan IP DNS punya google, yaitu : 8.8.8.8 dan 8.8.4.4. Lalu klik *Next*.
8. Selanjutnya akan muncul tampilan seperti dibawah ini : "*Setup has completed successfully*". Berarti *Wizard* DHCP *Server* telah selasai dan telah sukses lakukan. Lalu klik "OK".
9. Selanjutnya kalau buka menu : IP -> POOL maka akan ada IP Pool baru dengan nama "dhcp_pool".
10. Selanjutnya Tes Konfigurasi DHCP *Server* Menggunakan Laptop untuk mengakses internet apakah sudah *connect* atau belum.

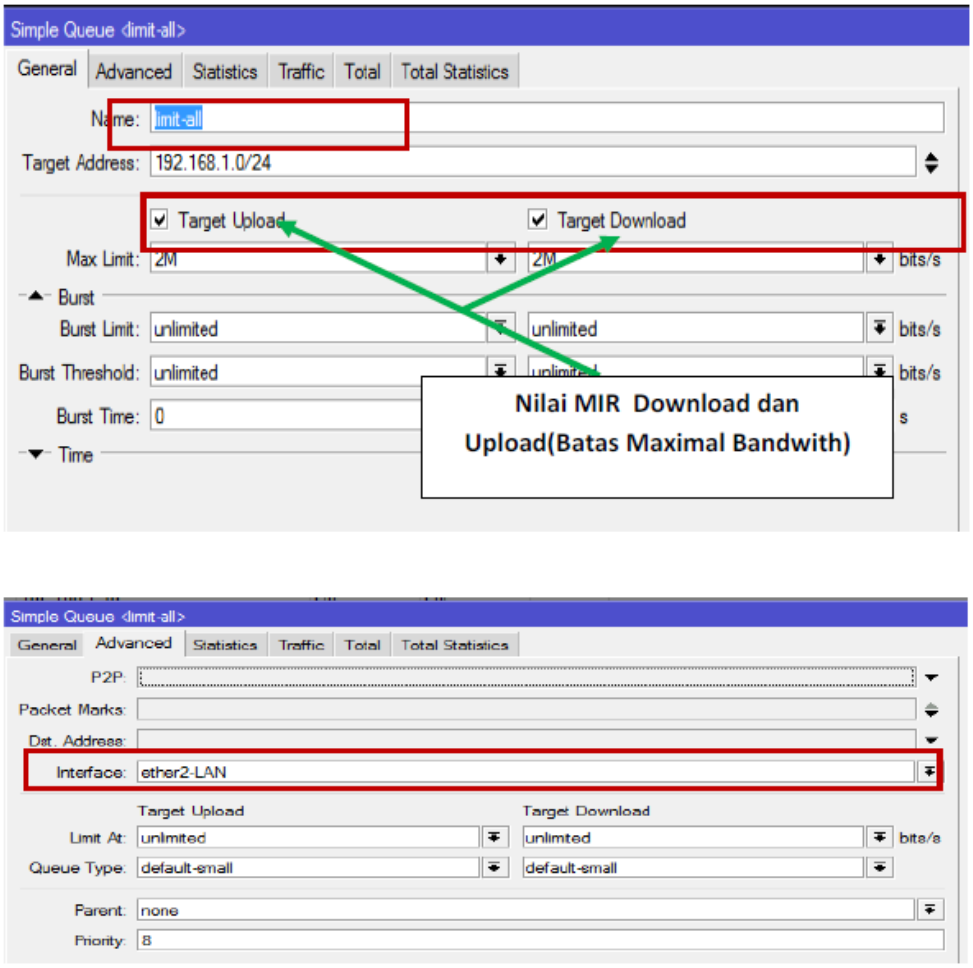
4.1.2 Proses Konfigurasi Management Bandwidth

Konfigurasi melalui syntak di Terminal :

queue simple add name="limit-all" target-addresses=192.168.1.0/24 interface=ether2-LAN max-limit=2M/2M

Konfigurasi melalui Winbox :

1. Kik Menu Queues dan pilih Simple Queue

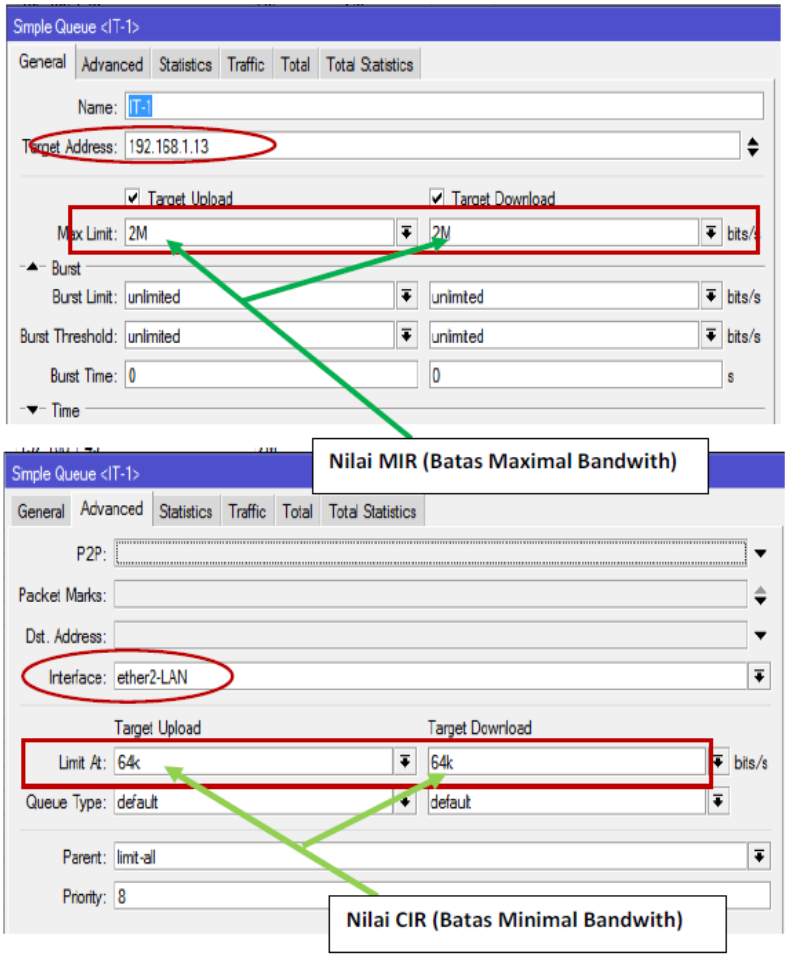


Gambar 4.4 Pemberian Nilai MIR Bandwidth

2. Konfigurasi *Bandwith Client* dengan mengatur Nilai CIR dn MIR yang akan didapat setiap user komputer. Konfigurasi CIR dan MIR untuk setiap client akan menggunakan konfigurasi pertama (Name=limit-all) sebagai induk *parent.*

Syntak

queue simple add name name="IT-1" target-ddresses=192.168.1.13/32 interface=ether2-LAN parent=limit-all limit-at=64k/64k max-limit=2M/2M

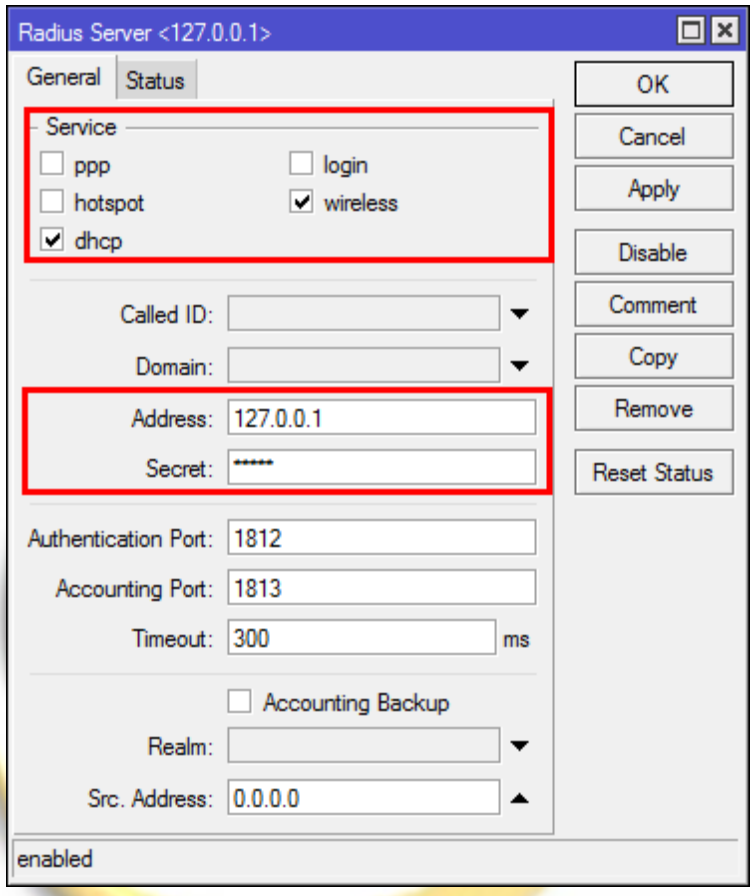


Gambar 4.5 Konfigurasi Bandwidth Client

4.1.3 Proses Konfigurasi Radius *Server*

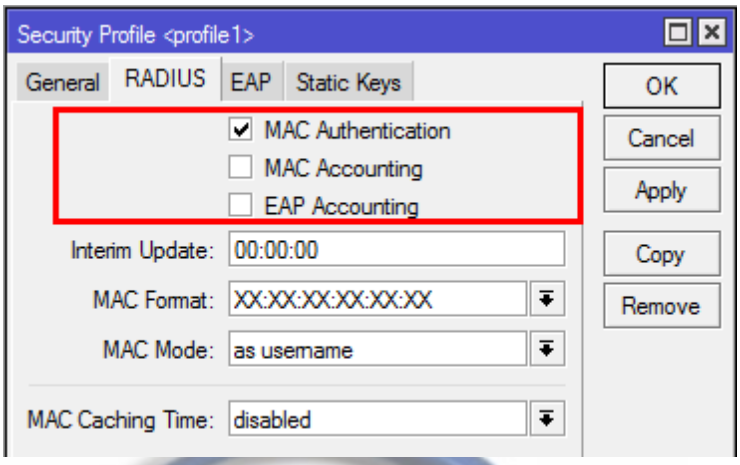
1. Pertama setting terlebih dahulu di sisi Router DHCP & Wireless sebagai Radius Client. Masuk ke menu "Radius". Centang opsi DHCP & Wireless, karena user DHCP dan user wireless yang nanti akan di-manage oleh *User Manager*. Pada opsi "*Address*", arahkan ke IP

address perangkat router utama yang menjalankan *service User Manager*.



Gambar 4.6 Konfigurasi Radius Server

2. Begitu juga pada *security profile* wireless, agar client wireless bisa di-manage oleh *User Manager*. Masuk ke menu Wireless --> klik Tab "*Security Profiles*". Buat Security Profiles baru, pada Tab RADIUS, klik opsi "MAC *Authentication*".



Gambar 4.7 Konfigurasi *Security Profiles*

3. Setting di-sisi Radius Client sudah selesai. Kemudian sekarang akan mulai setting di-sisi Radius Server *User Manager*. Tambahkan router radius client (Router DHCP & Wireless) pada *User Manager*. Masuk ke *web-base* user manager dengan alamat http://ip-router/userman Akan muncul halaman *login web-base User Manager, by default* bisa *login* dengan user *admin* password *kosong*. Di halaman itulah akan setting UserManager. Untuk menambahkan router radius client, masuk ke menu "Router", kemudian klik "Add".

4.1.4 Proses Konfigurasi Blokir Web Di Mikrotik

Pada cara ini detik akan di blok berdasarkan content langkahnya adalah sebagai berikut:

1. Login Menggunakan Winbox ke Router Mikrotik
2. Buka menu Terminal selanjutnya paste script dibawah ini

   /ip firewall filter add chain=forward content="detik.com"
   action=drop comment="Drop Detik"
   /ip firewall filter add chain=forward
   content="www.detik.com" action=drop comment="Drop Detik"

/ip firewall filter add chain=forward
content="apps.detik.com" action=drop comment="Drop Detik"
/ip firewall filter add chain=forward content="detik"
action=drop comment="Drop Detik"
/ip firewall filter add chain=forward content="detik."*
action=drop comment="Drop Detik"

4.1.5 Proses Konfigurasi Pengamanan Mikrotik Dari Serangan

1. Login ke Router dengan menggunakan winbox
2. klik "*New Terminal*". Ini akan membuka console mikrotik yang akan gunakan untuk melakukan konfigurasi. Script untuk mengamankan mikrotik dari port scanner, DDOS dan Netcut :

   add action=add-src-to-Address -list Address -list=DDOS Address -list-timeout=15m \ chain=input comment="" disabled=no dst-port=7331 protocol=tcp

   add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input comment="Port scanners to list " disabled=no protocol=tcp psd=21,3s,3,1

   add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input comment="SYN/FIN scan" disabled=no protocol=tcp tcp-flags=fin,syn

add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input comment="SYN/RST scan" disabled=no protocol=tcp tcp-flags=syn,rst

add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input disabled=no tcp-flags=fin,psh,urg,!syn,!rst,!ack protocol=tcp \ comment="FIN/PSH/URG scan"

add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input disabled=no protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg \ comment="ALL/ALL scan"

add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input

tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg comment="NMAP NULL scan" \ disabled=no protocol=tcp

add action=add-src-to-Address -list Address -list="port scanners" Address -list-timeout=2w \ chain=input comment="NMAP FIN Stealth scan" disabled=no protocol=tcp

add action=drop chain=input src-Address -list="port scanners"
add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

add action=accept chain=input comment="ANTI NETCUT" disabled=no dst-port=0-65535 \ protocol=tcp src-Address =192.168.1.2-192.168.1.254

4.2 PENGUJIAN

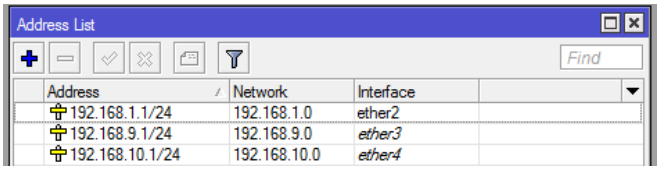
Gambaran umum tahap pengujian yang harus dilakukan sebagai berikut :

1. Pengujian Pengalmatan IP Address
2. Pengujian User Manager pada Radius Server
3. Kunci IP Address dan Mac Address di Mikrotik
4. Pengujian pengamanan DHCP dengan Protokol ARP
5. Pengujian blokir web tertentu di mikrotik
6. Mengamankan mikrotik dari serangan

4.2.1 Pengujian Pengalamatan IP *Address*

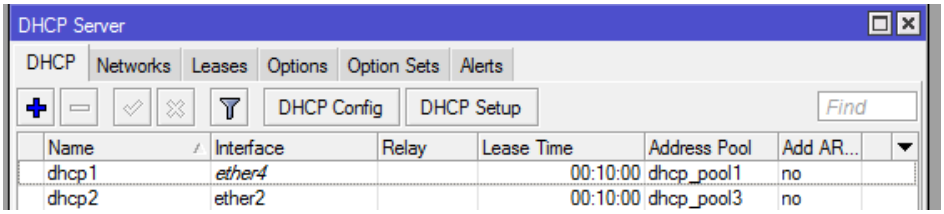
Setelah penulis melakukan konfigurasi alamat IP *Address* sesuai dengan *disegn* perancangan jaringan yang telah di buat oleh penulis. Untuk pengalamatan IP *Address* sebagai berikut :

1. Ether 2 192.168.1.1/24 DHCP
2. Ether 3 192.168.9.1/24 *Static*
3. Ether 4 192.168.10.1/24 DHCP



Gambar 4.8 Hasil Pemberian IP *Addrees* Pada Mikrotik

Untuk pemberian DHCP hanya pada Ether 2 dan Ether 4 sedangkan Ether 3 digunakan ada IP *Address static*



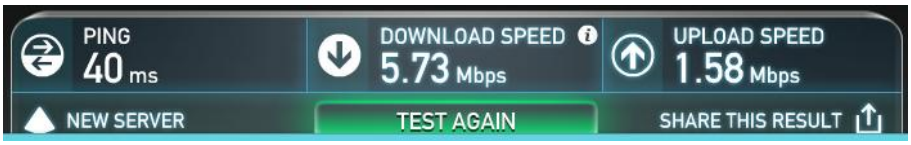
Gambar 4.9 Hasil Konfigurasi DHCP Pada *User*

4.2.2 Pengujian Management Bandwidth Di Mikrotik

Disini penulis mencoba membandingkan proses *user* melakukan *download* dan *upload* setelah dan sebelum penerapan manajemen *bandwidth*. Lalu penulis mencoba membadingkan *user* yang mendapatkan *unlimited download* dan *upload* dengan *user* yang telah mendapatkan jatah *download* dan *upload* setiap *user* sebesar *download* 1 Mbps dan *Upload* sebesar 1 Mbps dengan sumber internet melalui modem USB dengan vendor XL.

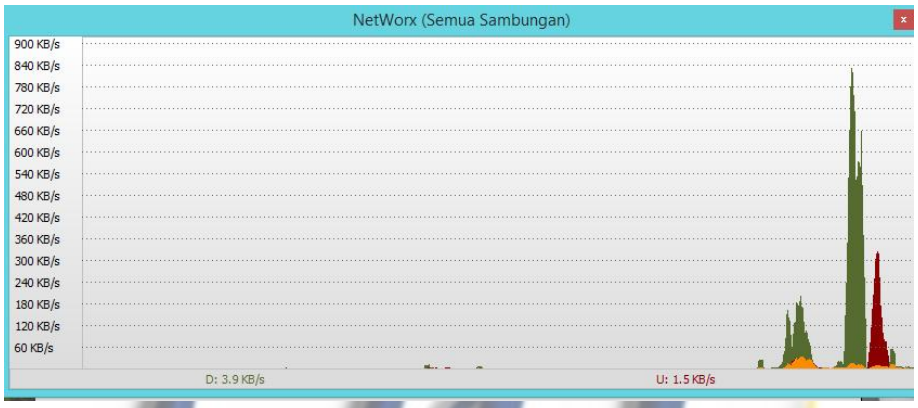
1. Gambaran Proses *Download* dan *Upload* Pada Umumnya

Gambar 4.10 dibawah hasil dari proses *download* dan *upload* tanpa menerapkan manajemen *bandwidth* pada *user* didapatkan *download* speed 5.73 Mbps dan *Upload* 1.58 Mbps sebagai alat testing menggunakan *Speedtest*.



Gambar 4.10 Pengetesan Hasil *Download* dan *Upload* Sebelum Penerapan Managemen *Bandwidth*

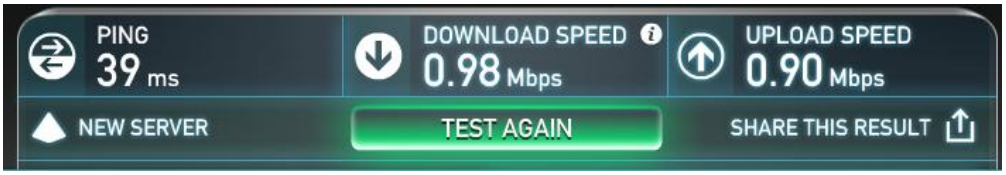
Dalam mengetasan pada Gambar 4.11 menggunakan *NetWorks* didapatkan proses *download* dan *upload* tidak stabil dan mengakibatkan akan terjadinya penggunaan internet pada *user* tidak lancar atau tidak stabil.



Gambar 4.11 Data *Download* dan *Upload* Sebelum Penerapan Managemen *Bandwidth*

2. *Download* dan *Upload* Dengan Mikrotik

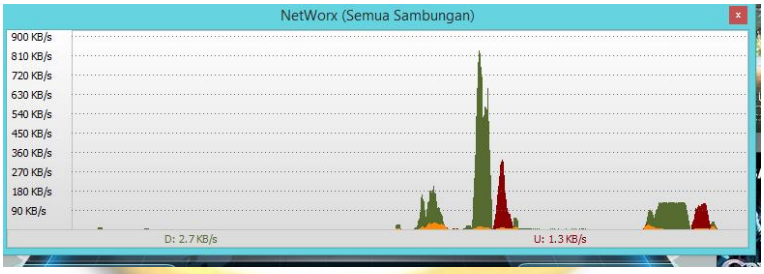
Gambar 4.12 hasil dari proses *download* dan *upload* yang telah menerapkan menerapkan manajemen *bandwidth* pada *user* didapatkan *download* speed 0.98 Mbps dan *Upload* 0.90 Mbps sebagai alat testing menggunakan *Speedtest.*



Gambar 4.12 Data *Download* dan *Upload* Sesudah Penerapan Managemen *Bandwidth*

Dari Gambar 4.13 dibawah dapat dibadingkan saat penerapan manajemen *bandwitd*h bahwa *user* yang tidak menerapkan manajemen *bandwidth* didapatkan grafik saat *user* melakukan proses *download* dan *upload* tidak stabil berbeda jauh saat *user* menerapkan manajemen *bandwidth* pada jaringan komputernya, sehingga manfaat penerapakan manajemen *bandwidth* pada suatu jaringan adalah :

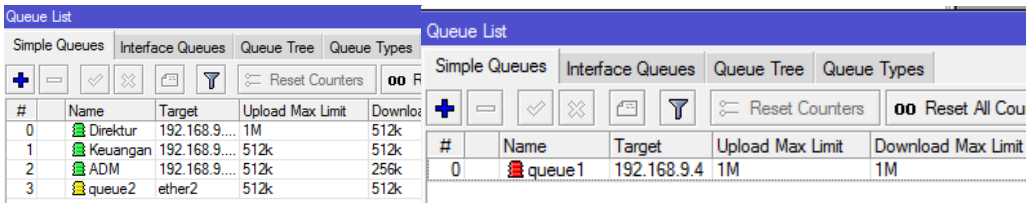
1. Semua komputer dapat menggunakan internet dengan lancar dan stabil walaupun semua unit komputer menggunakan internet dalam waktu yang bersamaan.
2. Semua bagian unit komputer mendapatkan *bandwidth* sesuai dengan kebutuhan koneksi internet.
3. Memaksimalkan *bandwidth* di semua unit komputer.
4. Membantu admin dalam mengontrol *bandwidth*.



Gambar 4.13 Grafik Data *Download* dan *Upload* Setelah Penerapan Managemen *Bandwidth*

3. Penjelasan Manajemen *Bandwidth* Yang Di Terapkan

Disini penulis mencoba melakukan pengujian kepada *user* proses *download* dan *upload*. Hasil pengujian dijelaskan pada Gambar 4.14.



Gambar 4.14 Hasil Pembatasan Bandwith

Pada Gambar 4.14 diatas terlihat *user* queue1 telah melewati batas *bandwidth* yang ditentukan sehingga mikrotik memberi warna merah namun pada *user* queue 2 berwarna kuning artinya *user* tersebut mendekati *bandwidth* yang telah ditentukan lalu pada *user* Direktur, Keuangan, ADM terlihat mikrotik masih memberi peringatan hijau artinya *user* masih dalam batas aman dari yang telah ditentukan

Warna merah : pemakaian *bandwidth* berkisar 86% - 100 %

Warna kuning : pemakaian *bandwidth* berkisar 51% - 85%

Warna hijau : Pemakaian *bandwidth* berkisar 0% - 50%

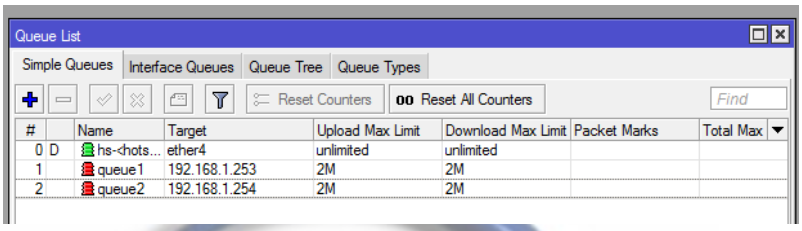
4. Management *Bandwidth* Skala Pioritas

Dengan adanya pioritas, maka *user* akan mendapatkan alokasi *bandwidth* yang lebih dibandingkan *user* lain, selama tidak mengganggu nilai CIR dari *user* – *user* yang lain. Router Mikrotik memberikan skala pioritas dengan nilai "1" sampai "8", dengan nilai "1" sebagai pioritas tertinggi menyusul nilai berikutnya hingga nilai "8" sebagai nilai pioritas paling rendah.

Pada skenario yang digunakan adalah sebagai berikut :

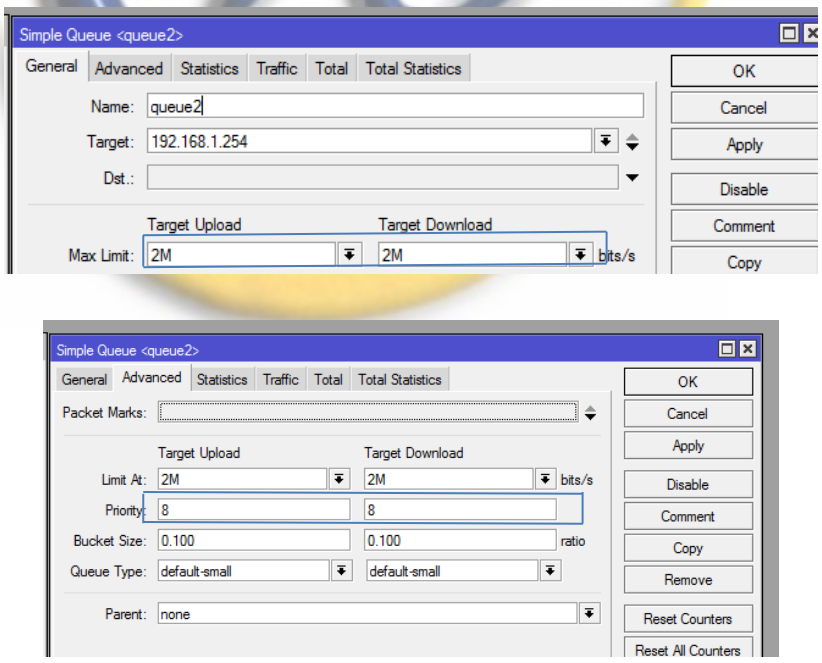
1. *User* 1 yaitu queue 2 memiliki pioritas 8
2. *User* 2 yaitu queue 1 memiliki pioritas 1

Lalu skenario berikutnya penulis melakukan pengetesan *download* dan *upload* terhadap ke 2 *user* tersebut secara bersamaan sehingga mendekati batas *bandwidth* yang telah ditentukan denga bukti adanya symbol warna merah dijelaskan pada gambar 4.15 di bawah ini.



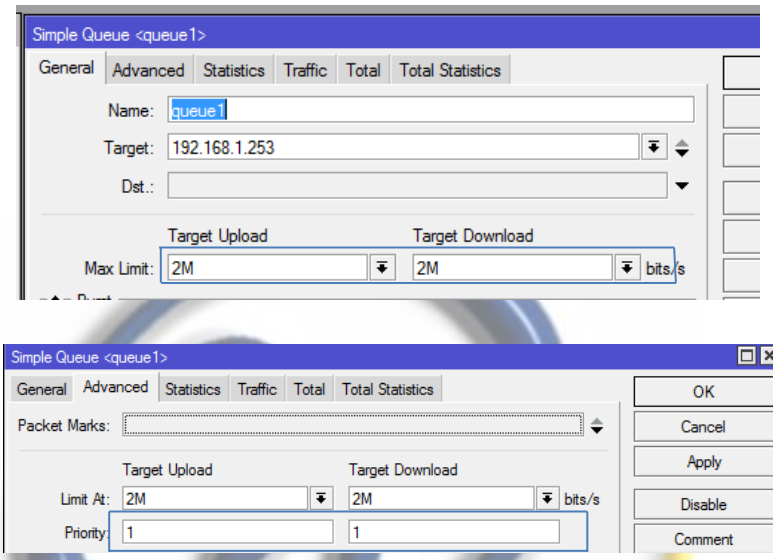
Gambar 4.15 *Test Trafik User*

Dibawah ini pada Gambar 4.16 *user* 1 di berikan jatah max *download* sebanyak 2 MB dan max *upload* sebanyak 2 MB dengan pioritas nilai "8".



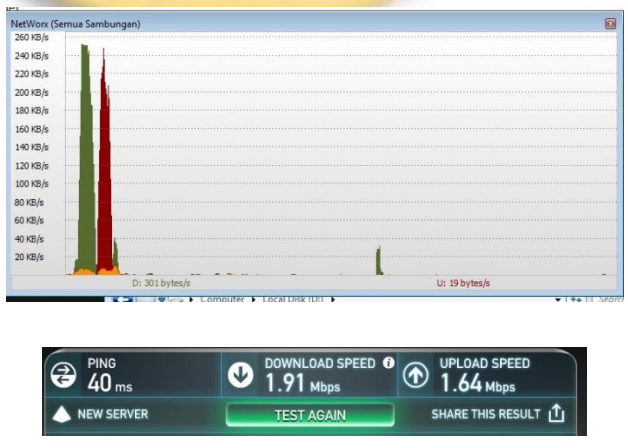
Gambar 4.16 Konfigurasi Manajemend *Bandwidth* Pioritas Pada *User* 1

Dibawah ini pada Gambar 4.17 *user* 2 di berikan jatah maksimal *download* sebanyak 2 MB dan maksimal *upload* sebanyak 2 MB dengan pioritas nilai "1".



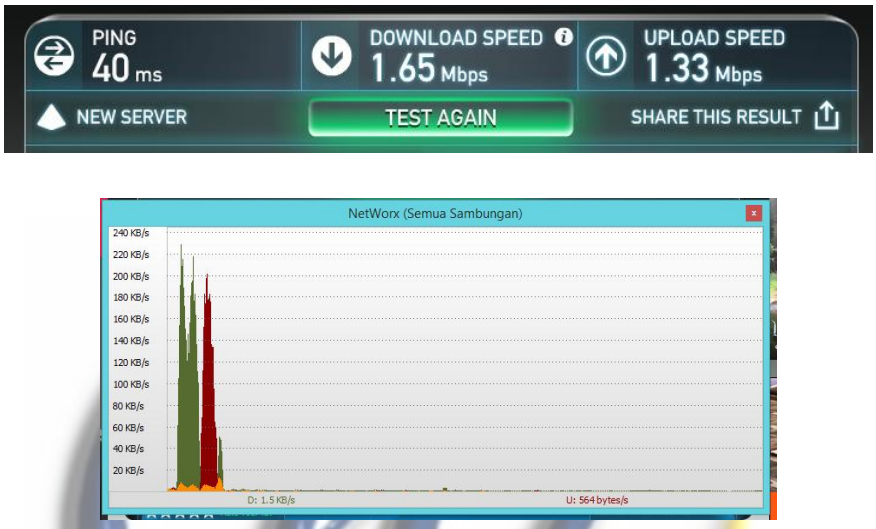
Gambar 4.17 Konfigurasi Manajemend *Bandwidth* Pioritas di *User* 2

Pada hasil mengetesan pada *user* 2 didapatkan *Download* Speed sebanyak 1.91 Mbps dan *Upload* sebnyak 1.64 Mbps dijelaskan pada Gambar 4.18.



Gambar 4.18 Hasil Test Managemen *Bandwidth* Pioritas pada *User* 2

Pada hasil mengetesan pada *user* 1 didapatkan *Download Speed* sebanyak 1.65 Mbps dan *Upload* sebnyak 1.33 Mbps dijelaskan pada Gambar 4.19.



Gambar 4.19 Hasil Test Managemen *Bandwidth* Pioritas pada *User* 1

Kesimpulan didapatkan bahwa *user* 2 yang memperoleh pioritas nilai "1" mendapatkan jatah Maksimal *Download* dan Maksimal *Upload* lebih bessar dibandingkan pada *user* 1 yang memperoleh pioritas nilai "8".

5. Hasil Implementasi *Managemend Bandwidth*

Disini penulis melakukan implementasi management bandwidth untuk inputan jaringan berasal dari Ether 2 pada jaringan komputer di Rumah Sakit Khusus Ibu dan Anak Kota Bandung didapat beberapa data hasil dari penelitian tersebut dapat dijelaskan pada Tabel 4.1 sebagai berikut.

Tabel 4.1 Data Monitoring Bandwidth

No	Ruangan	IP Address	Tanpa Management Bandwidth		Dengan Management Bandwidth	
			Donwload	***Upload***	***Download***	***Upload***
1	Basement	192.168.1.10	15.79 Mbps	226.22 Kbps	1.78 Mbps	1.71 Mbps
2	Basement	192.168.1.11	7.23 Mbps	133.13 Kbps	1.7 Mbps	112.13 Kbps
3	Basement	192.168.1.12	3.22 Mbps	199.08 Kbps	1.23 Mbps	1.08 Mbps
4	Basement	192.168.1.13	2.00 Mbps	44.03 Kbps	1.62 Mbps	1.03 Mbps
5	Basement	192.168.1.14	2.10 Mbps	112.98 Kbps	1.71 Mbps	1.08 Mbps
6	Basement	192.168.1.15	1.08 Mbps	111.92 Kbps	1.22 Mbps	1.92 Mbps
7	Basement	192.168.1.16	1.03 Mbps	127.87 Kbps	1.34Mbps	221.07 Kbps
8	Basement	192.168.1.17	1.98 Mbps	221.82 Kbps	1.29 Mbps	1.02 Kbps
9	Basement	192.168.1.18	1.92 Mbps	181.77 Kbps	1.24 Mbps	119.70 Kbps
10	Basement	192.168.1.19	1.87 Mbps	119.71 Kbps	1.19 Mbps	1.71 Mbps
11	Base G	192.168.1.20	1.82 Mbps	1.66 Mbps	1.13 Mbps	121.66 Kbps
12	Base G	192.168.1.21	3.96 Mbps	1.61 Mbps	1.08 Mbps	331.61 Kbps
13	Base G	192.168.1.22	5.85 Mbps	2.56 Mbps	1.03 Mbps	1.56 Mbps
14	Base G	192.168.1.23	7.74 Mbps	1.51 Mbps	1.98 Mbps	1.51 Mbps
15	Base G	192.168.1.24	9.63 Mbps	1.45 Mbps	1.92 Mbps	1.45 Mbps
16	Base G	192.168.1.25	28.88 Mbps	342.99 Kbps	1.88 Mbps	1.66 Mbps
17	Base G	192.168.1.26	1.42 Mbps	112.35 Kbps	1.82 Mbps	451.35 Kbps
18	Base G	192.168.1.27	5.31 Mbps	130.30 Kbps	1.77 Mbps	221.30 Kbps
19	Base G	192.168.1.28	1.20 Mbps	222.24 Kbps	1.71 Mbps	1.24 Mbps
20	Base G	192.168.1.29	9.09 Mbps	225.19 Kbps	1.66 Mbps	1.19 Mbps
21	Base G	192.168.1.30	2.98 Mbps	310.74 Kbps	1.61 Mbps	1.67 Mbps
22	Base G	192.168.1.31	22.87 Mbps	119.72 Kbps	1.56 Mbps	1.7 Mbps
23	Base G	192.168.1.32	4.76 Mbps	1123.69 Kbps	1.51 Mbps	1.23 Mbps
24	Base G	192.168.1.33	6.65 Mbps	111.67 Kbps	1.45 Mbps	1.62 Mbps
25	Base 1	192.168.1.34	2.54 Mbps	1.64 Kbps	1.40 Mbps	1.71 Mbps
26	Base 1	192.168.1.35	18.333 Mbps	2.96 Kbps	1.35 Mbps	1.22 Mbps
27	Base 1	192.168.1.36	2.32 Mbps	1.60 Kbps	1.92 Mbps	1.22 Mbps
28	Base 2	192.168.1.37	7.19 Mbps	201.04 Kbps	1.24 Mbps	1.29 Mbps
29	Base 2	192.168.1.38	6.10 Mbps	1.55 Mbps	1.19 Mbps	1.24 Mbps
30	Base 2	192.168.1.39	7.99 Mbps	1.53 Mbps	1.67 Mbps	1.01 Mbps
31	Base 3	192.168.1.40	8.98 Mbps	128.18 Kbps	1.78 Mbps	1.22 Mbps

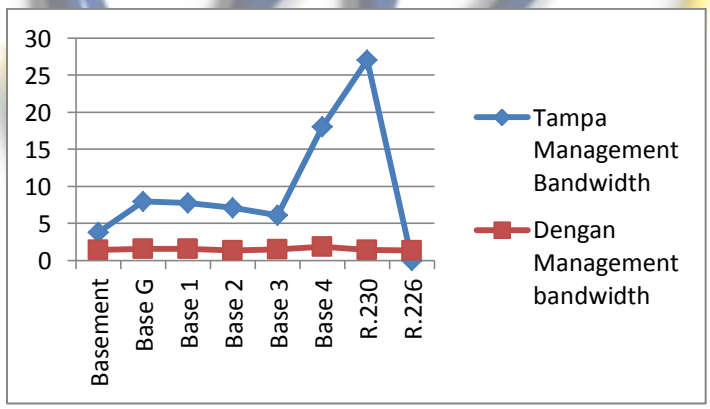
32	Base 3	192.168.1.41	4.77 Mbps	111.48 Kbps	1.41 Mbps	1.08 Mbps
33	Base 3	192.168.1.42	3.66 Mbps	124.45 Kbps	1.41 Mbps	1.03 Mbps
34	Base 3	192.168.1.43	5.55 Mbps	120.43 Kbps	1.41 Mbps	1.98 Mbps
35	Base 3	192.168.1.44	7.44 Mbps	119.41 Kbps	1.40 Mbps	1.92 Mbps
36	Base 4	192.168.1.45	18.06 Mbps	312.33 Kbps	1.88 Mbps	1.71 Mbps
37	R.226	192.168.1.46	5.22 Kbps	1.36 Kbps	1.40 Mbps	1.82 Mbps
38	R.226	192.168.1.47	5.11 Kbps	1.34 Kbps	1.39 Mbps	1.77 Mbps
39	R.226	192.168.1.48	5.01 Kbps	1.31 Kbps	1.39 Mbps	451.71 Kbps
40	R.226	192.168.1.49	7.74 Kbps	8.07 Kbps	1.39 Mbps	1.66 Mbps
41	R.226	192.168.1.50	6.79 Kbps	1.27 Kbps	1.38 Mbps	221.61 Kbps
42	R.226	192.168.1.51	6.68 Kbps	1.24 Kbps	1.38 Mbps	1.56 Mbps
43	R.226	192.168.1.52	6.57 Kbps	1.22 Kbps	1.38 Mbps	221.51 Kbps
44	R.226	192.168.1.53	6.46 Kbps	1.19 Kbps	1.38 Mbps	111.45 Kbps
45	R.226	192.168.1.54	6.35 Kbps	1.17 Kbps	1.37 Mbps	1.41 Mbps
46	R.226	192.168.1.55	6.24 Kbps	1.15 Kbps	1.37 Mbps	451.41 Kbps
47	R.226	192.168.1.56	7.13 Kbps	1.12 Kbps	1.37 Mbps	1.40 Mbps
48	R.226	192.168.1.57	2.02 Kbps	1.10 Kbps	1.36 Mbps	1.40 Mbps
49	R.226	192.168.1.58	3.91 Kbps	1.08 Kbps	1.36 Mbps	1.40 Mbps
50	R.226	192.168.1.59	7.30 Kbps	1.05 Kbps	1.70 Mbps	1.77 Mbps
51	R.226	192.168.1.60	7.69 Kbps	1.03 Mbps	1.35 Mbps	1.39 Mbps
52	R.230	192.168.1.61	9.58 Mbps	1.00 Mbps	1.35 Mbps	221.39 Kbps
53	R.230	192.168.1.62	1.47 Mbps	0.98 Mbps	1.35 Mbps	1.38 Mbps
54	R.230	192.168.1.63	8.36 Mbps	0.96 Mbps	1.34 Mbps	221.38 Kbps
55	R.230	192.168.1.64	5.25 Mbps	0.93 Mbps	1.34 Mbps	1.38 Mbps
56	R.230	192.168.1.65	7.14 Mbps	0.91 Mbps	1.34 Mbps	331.38 Kbps
57	R.230	192.168.1.66	9.03 Mbps	0.89 Mbps	1.33 Mbps	1.37 Mbps
58	R.230	192.168.1.67	9.92 Mbps	0.86 Mbps	1.33 Mbps	122.37 Kbps
59	R.230	192.168.1.68	97.80 Mbps	1,55 Mbps	1.90 Mbps	1.56 Mbps
60	R.230	192.168.1.69	94.70 Mbps	0.81 Mbps	1.33 Mbps	111.36 Kbps

Pada Tabel 4.2 merupakan data dari rata-rata pemakain bandwidth untuk dipakai *download* dan *upload* di RSKIA Kota Bandung

Tabel 4.2 Perbandingan Rata- Rata *Bandwidth* Pada User

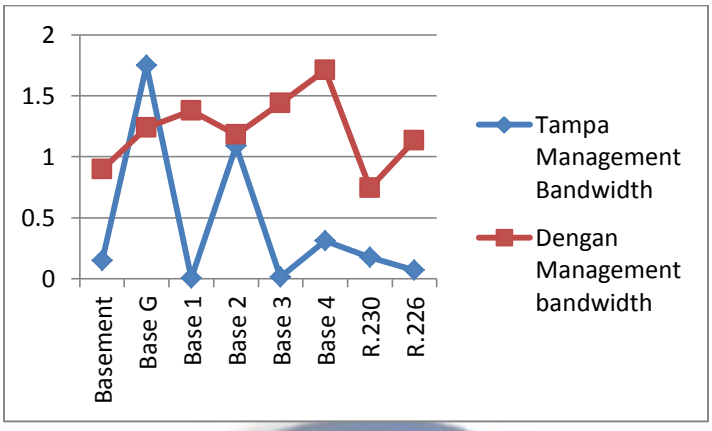
Ruangan	Tanpa Management Bandwidth		Dengan Management Bandwidth	
	Donwload	***Upload***	***Download***	***Upload***
Basement	3.82 Mbps	0.147 Mbps	1.43 Mbps	0.898 Mbps
Base G	8.01 Mbps	1.75 Mbps	1.57 Mbps	1.24 Mbps
Base 1	7.73 Mbps	0.002 Mbps	1.55 Mbps	1.38 Mbps
Base 2	7.09 Mbps	1.09 Mbps	1.36 Mbps	1.18 Mbps
Base 3	6.08 Mbps	0.012 Mbps	1.48 Mbps	1.44 Mbps
Base 4	18.06 Mbps	0.312 Mbps	1.88 Mbps	1.71 Mbps
R.230	27.02 Mbps	0.173 Mbps	1.40 Mbps	0.744 Mbps
R.226	0.006 Mbps	0.070 Mbps	1.39 Mbps	1.135 Mbps

Pada Gambar 4.20 merupakan data dari rata- rata *download* di RSKIA Kota Bandung



Gambar 4.20 Data Rata-Rata *Download*

Pada Gambar 4.21 merupakan data dari rata- rata *upload* di RSKIA Kota Bandung



Gambar 4.21 Data Rata-Rata *Upload*

Pada Gambar 4.20 dan Gambar 4.21 dijelaskan trafik pada diagram grafik tampa management bandwidth setiap user terjadi ketidak seimbangan *bandwidth* yang didapatkan oleh user berbeda dengan grafik user yang telah menerapkan management *bandwidth* pada user yang telah menerapkan management *bandwidth* setiap user mendapatkan hampir rata dalam penerimaan bandwidh. Pada user yang menerapkan management bandwidth setiap user diberi batas maksimal baik *bandwidth download* dan *upload* sebanyak 2 Mbps untuk yang tidak menerapkan management *bandwidth* mendapatkan batas maksimal *bandwidth download* dan *upload* sebanyak *unlimited.*

Pada Tabel 4.3 Merupakan data monitoring Bandwidth yang pemakaiannya terbesar.

Tabel 4.3 Perbandingan *Bandwidth* Pada User

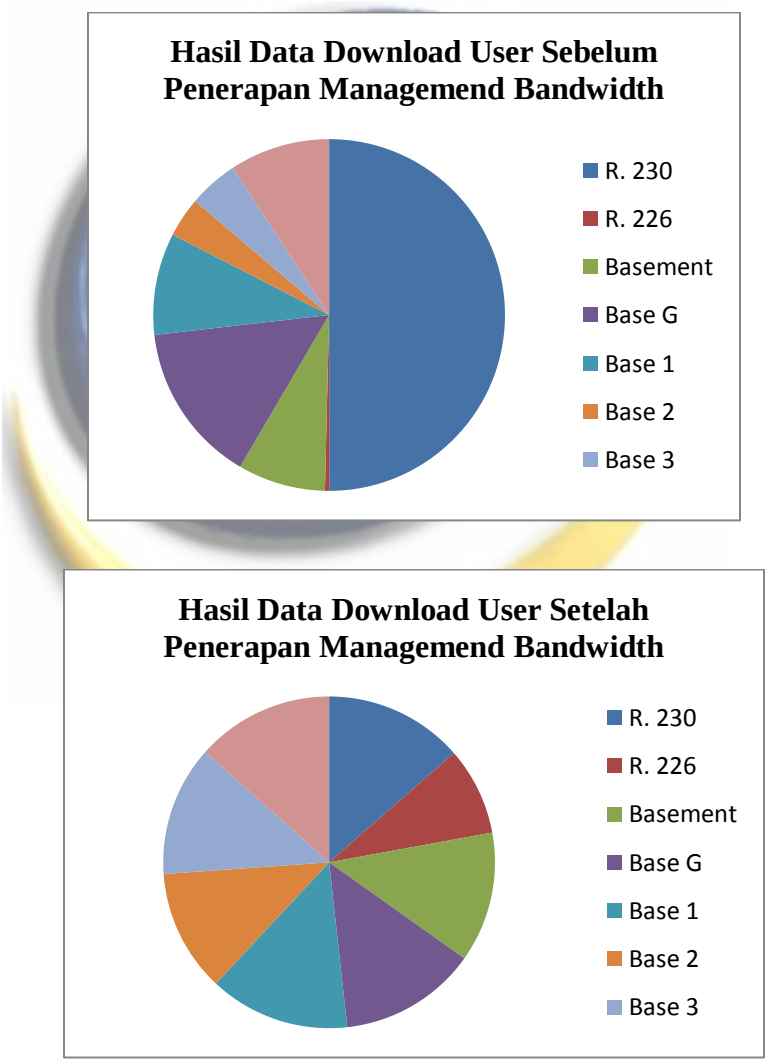
No	**Ruangan**	**IP Address**	**Tanpa Management *Bandwidth***		**IP Address**	**Dengan Management *Bandwidth***	
			Download	***Upload***		***Download***	***Upload***
1	R. 230	192.168.1 .68	97,88 Mbps	1,55 Mbps	192.168.1 .68	1,90 Mbps	1,56 Mbps

2	R. 226	192.168.1.49	7,74 Kbps	8,07 Kbps	192.168.1.59	1,70 Mbps	1,77 Mbps
3	Basement	192.168.1.10	15,79 Mbps	261,22 Kbps	192.168.1.10	1,78 Mbps	1.71 Kbps
4	Ruang G	192.168.1.25	28,88 Mbps	342,94 Kbps	192.168.1.25	1,88 Mbps	1,66 Mbps
5	Base 1	192.168.1.35	18,33 Mbps	296,99 Kbps	192.168.1.36	1,92 Mbps	1,22 Mbps
6	Base 2	192.168.1.37	7,19 Mbps	201,04 Kbps	192.168.1.38	1,67 Mbps	1,01Mbps
7	Base 3	192.168.1.40	8,92 Mbps	128,18 Kbps	192.168.1.40	1,78 Mbps	1,22Mbps
8	Base 4	192.168.1.45	18,06 Mbps	312,33 Kbps	192.168.1.45	1,88 Mbps	1,71 Mbps

Pada Tabel 4.1 didapatkan data hasil monitoring jaringan untuk *download* di RSKIA Kota Bandung Tanpa management bandwidth bahwa untuk ruangan yang pemakaian *bandwidth* untuk meng*download* adalah di ruang 230 sedangkan ruangan yang sedikit dalam menggunakan *bandwidth* untuk meng*download* adalah ruangan 226 lalu data hasil monitoring jaringan untuk *upload* di RSKIA Kota Bandung bahwa untuk ruangan yang pemakaian *bandwidth* untuk meng*upload* adalah di ruang 230 sedangkan ruangan yang sedikit dalam menggunakan *bandwidth* untuk *upload* adalah ruangan Base 3.

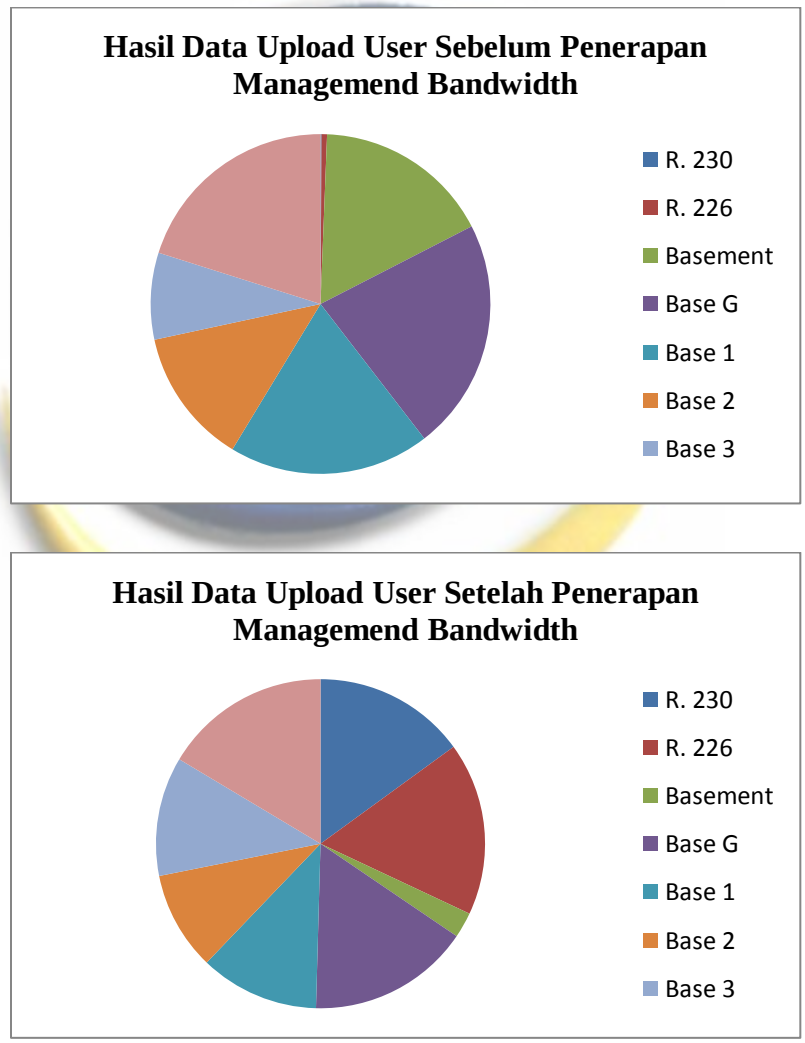
Sedangkan setelah melakukan *management bandwidth* didapatkan maksimal *download* terdapat pada Ruang 230 sebesar 1,90 Mbps sedangkan untuk *upload* paling besar terdapat pada Base 4 sebesar 1,71 Mbps.

Pada Gambar 4.22 dapat dibandingkan pada diagram lingkaran bahwa hasil data *download* pada *user* sebelum penerapan management bandwidth setiap user pada satu jaringan mendapatkan trafik *download* yang berbeda tiap unitnya sedangkan setelah setelah penerapan *management bandwidth* dapat dilihat pada Gambar 4.22 setiap user dalam satu jaringan hampir mendapatkan trafik *download* yang hampir sama.



Gambar 4.22 Perbandingan Data *Download* User

Pada Gambar 4.23 dapat dibandingkan pada diagram lingkaran bahwa hasil data *upload* pada *user* sebelum penerapan management bandwidth setiap user pada satu jaringan mendapatkan trafik *upload* yang berbeda tiap unitnya sedangkan setelah setelah penerapan *management bandwidth* dapat dilihat pada Gambar 4.23 setiap *user* dalam satu jaringan hampir mendapatkan trafik *upload* yang hampir sama.



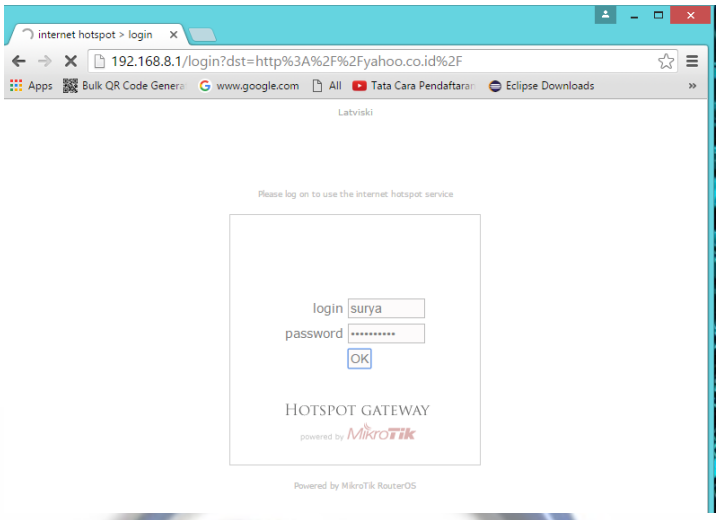
Gambar 4.23 Perbandingan Data *Upload* User

Kesimpulan setelah menerapkan *managemend bandwidth* trafik jaringan menjadi stabil tidak adanya perbedaan yang mencolok karena setiap *user* mendapatkan jatah masing- masing maksimal *bandwidth* dan *upload* sebesar 2 Mbps.

4.2.3 Pengujian User Manager Pada Radius *Server*

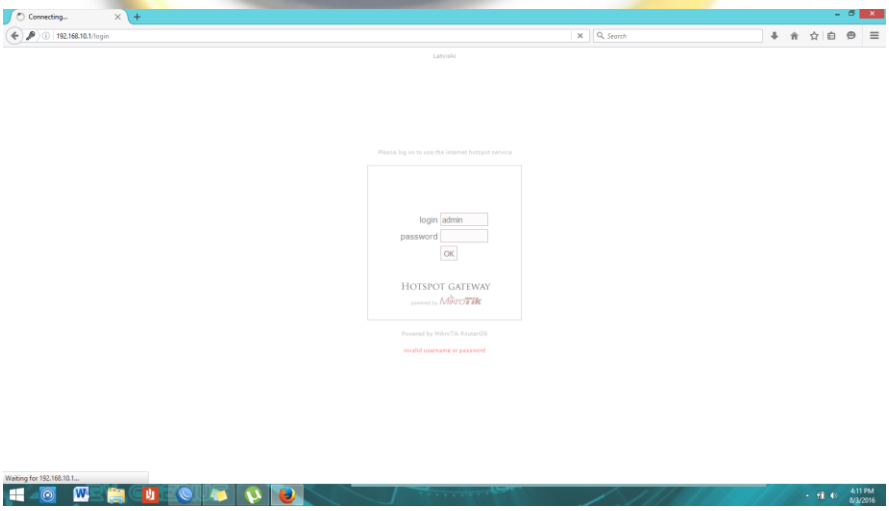
Pada suatu jaringan wireless memiliki kelebihan dimana penguna dapat dengan mudah masuk ke dalam sistem jarinan. Jika seorang *user* sudah mendeteksi adanya signal wireless maka *user* tersebut dapat denga mudah menghubungkan laptop atau *smartphone* yang dimiliknya sehingga terhubung kejaringan wireless. Tentunya kemudahan ini sedikit berbeda pada jaringan kabel dimana *user* harus membanguna akses fisik kabel untuk masuk ke jaringan maka dengan ini selaku Administrator jaringan harus memberikan perhatian lebih terhadap kases yang akan diberikan kepada *user* tersebut.

Oleh karena itu langkah yang tepat adalah membatasi akses *user* yang akan masuk kesuatu jaringan komputer dengan menerapkan Radius *Server* . Dibawah ini setiap *user* yang akan masuk kedalam suatu jaringan mempunyai *username* dan *password* masing masing dan tidak akan bisa dalam satu jaringan ada *username* dan *password* yang sama dalam satu jaringan.



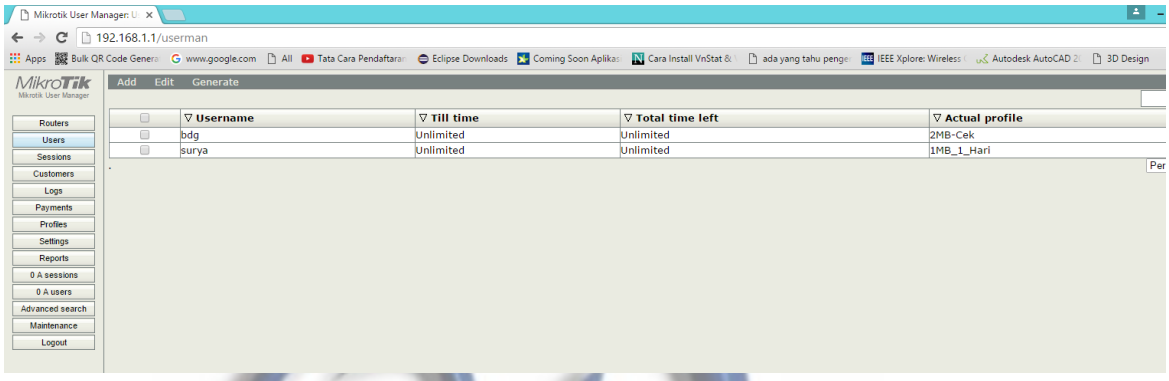
Gambar 4.24 Login Masuk Radius *Server*

Namun apabila ada *user* yang akan masuk kedalam suatu jaringan salah memasuki *username* dan *password* salah maka Radius *Server* memberi peringatan bahwa *username* dan *password* yang dimasukin tidak sesuai dengan *username* dan *password* yang telah di daftarkan pada radius *Server* seperti Gambar 4.25.



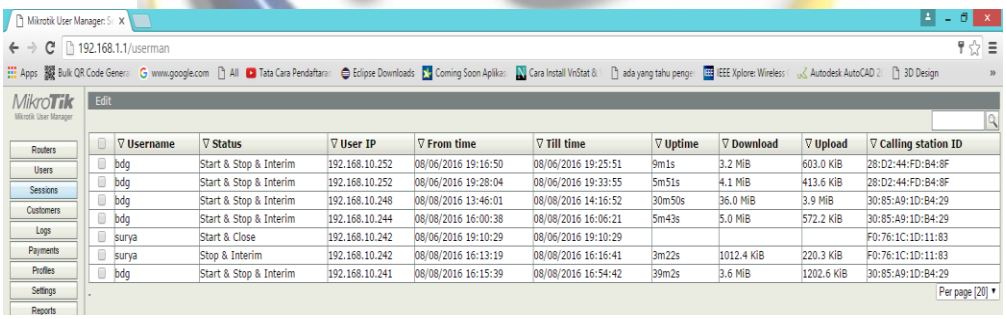
Gambar 4.25 Salah Memasuki Login Pada Radius *Server*

Disini pada Gambar 4.26 merupakah contoh *list* yang telah terdaftar pada Radius *Server* sehingga *user* yang telah terdaftar dapat melakukan akses ke jaringan komputer .



Gambar 4.26 *List User* Yang Telah Terdaftar

Pada Gambar 4.27 di Radius *Server* seorang Admin Jaringan dapat mengetahui jumlah pemakaian *Download* dan *upload* tiap *user.*

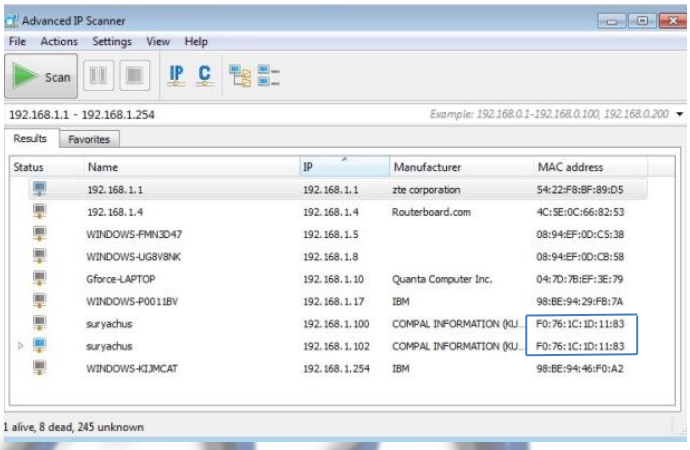


Gambar 4.27 Jumlah Pemakaian *Download* dan *Upload* Tiap User

4.2.4 Pengujian Penguncian IP *Address* Dengan Mac *Address*

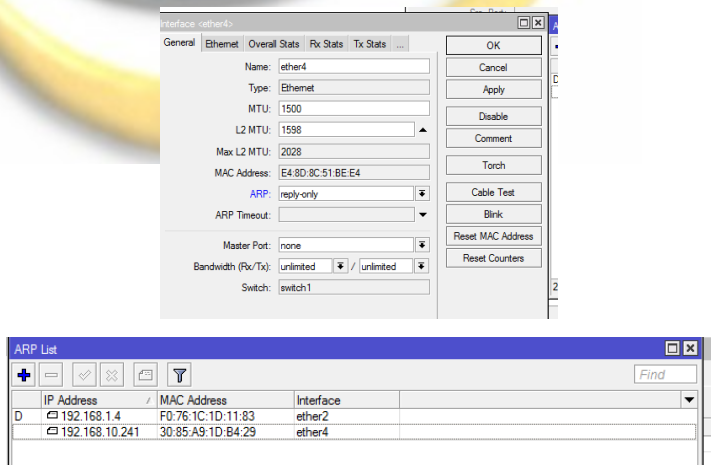
Didalam suatu jaringan komputer sering terjadi *user* yang memiliki keahlian yang lebih dalan jaringan komputer yang berusaha masuk kedalam suatu jaringan komputer dengan cara ikut mengsamakan IP *Address* atau Mac *Addrees* sehingga sering terjadi adanya 2 alamat

Mac *Address* yang sama alamat satu jaringan namun dengan IP *Address* berbeda maupun sebaliknya seperti pada Gambar 4.28.



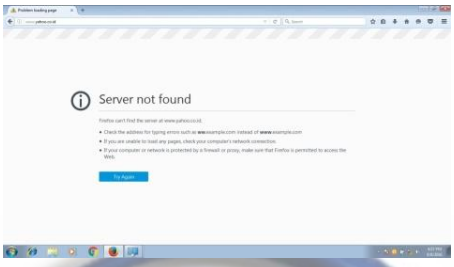
Gambar 4.28 Mac *Address* Yang *Double*

Disini penulis pada Gambar 4.29 melakukan konfigurasi mengunci IP *Address* dengan Mac *Address* nya sehingga setiap Mac *Address* mendapatkan IP *Address* yang sama dan IP *Address* tersebut tidak akan diberikan kepad Mac *Address* yang lain.



Gambar 4.29 Proses Kunci IP *Address* Dan Mac *Address* *User* Di Mikrotik

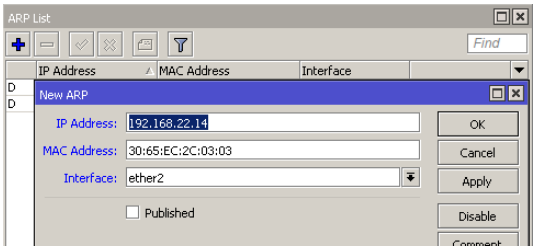
Sehingga apabila ada *user* yang memasukan Mac *Address* Clon atau Mac *Address* Changer maka *user* tersebut tidak akan dapat masuk ke dalam jaringan komputer tersebut seperti gambar 4.30 dibawah ini.



Gambar 4.30 *User* yang Tidak Dapat Masuk Jaringan Dengan Mac *Address* Clon

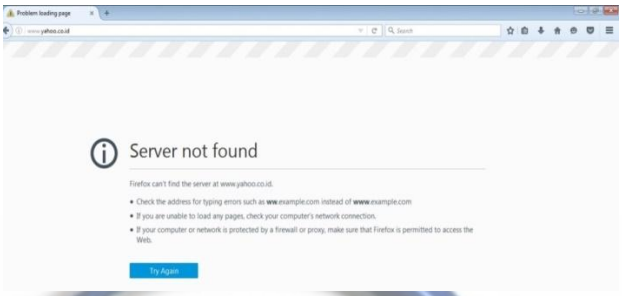
4.2.5 Pengujian Pengamanan DHCP Dengan Protokol ARP

Disini penulis mencoba menambahkan pengamanan pada DHCP dengan protocol ARP yang funginya dengan mengubah interface ARP di interface yang mengarah ke jaringan local ke reply-only maka router mikrotik hanya akan merespon request dari *user* yang IP dan Mac *Address* nya sudah terdaftar di ARP list saja sehingga apabila ada *user* yang masuk atau menambah PC di jaringan local meskipun sudah terkoneksi menggunakan kabel LAN dan sudah set IP static tetap tidak akan terkoneksi ke jaringan (internet), *user* dapat terkoneksi dengan menginput IP & Mac *Address* PC tersebut di ARP *list*



Gambar 4.31 Proses Mendaftarkan *User* di ARP List

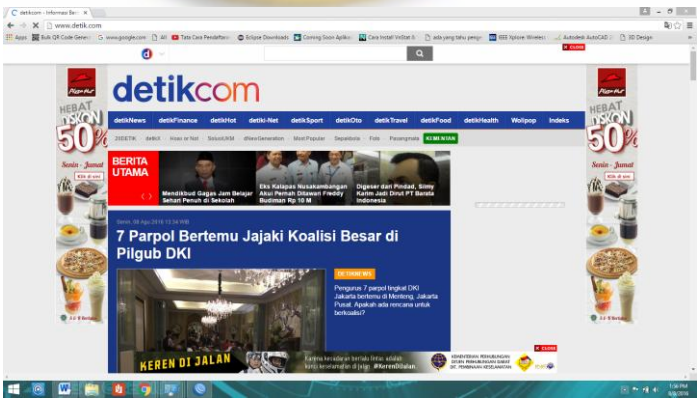
Jika *user* didalam jaringan yang mengubah IP dari DHCP ke statik maka router tidak akan menanggapinya seperti Gambar 4.30 dibawah ini.



Gambar 4.32 Mikrotik Tidak akan memberikan Akses

4.2.6 Pengujian Blokir Web Tertentu Di Mikrotik

Disini penulis mencoba melakukan blokir website tertentu di internet sehingga setiap *user* pada suatu jaringan yang terhubung saat akan membuka website yang telah ditentukan akan di blokir maka *user* tidak akan bisa membuka website tersebut. Disini penulis mencoba memblokir alamat Detik.com sehingga *user* tidak dapat mengakses halaman detik.com. pada Gambar 4.33 ini tampilan web browser masih dapat membuka halaman detik.com.

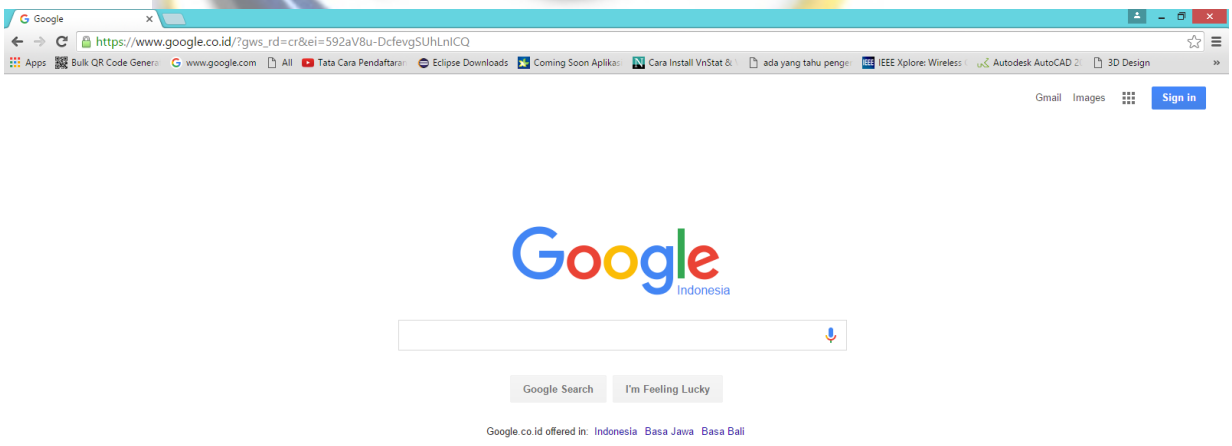


Gambar 4.33 Tampilan Detik.com Sebelum Diblokir

Setelah diaktifkan rull pada mikrotik yang membuat *user* tidak dapat mengakses halaman Detik.com maka pada tampilan layar pada web browser akan menampilkan "*Error: Forbidden*" seperti Gambar 4.34 dibawah ini.

Gambar 4.34 Tampilan Detik.com Yang Telah Di Blokir

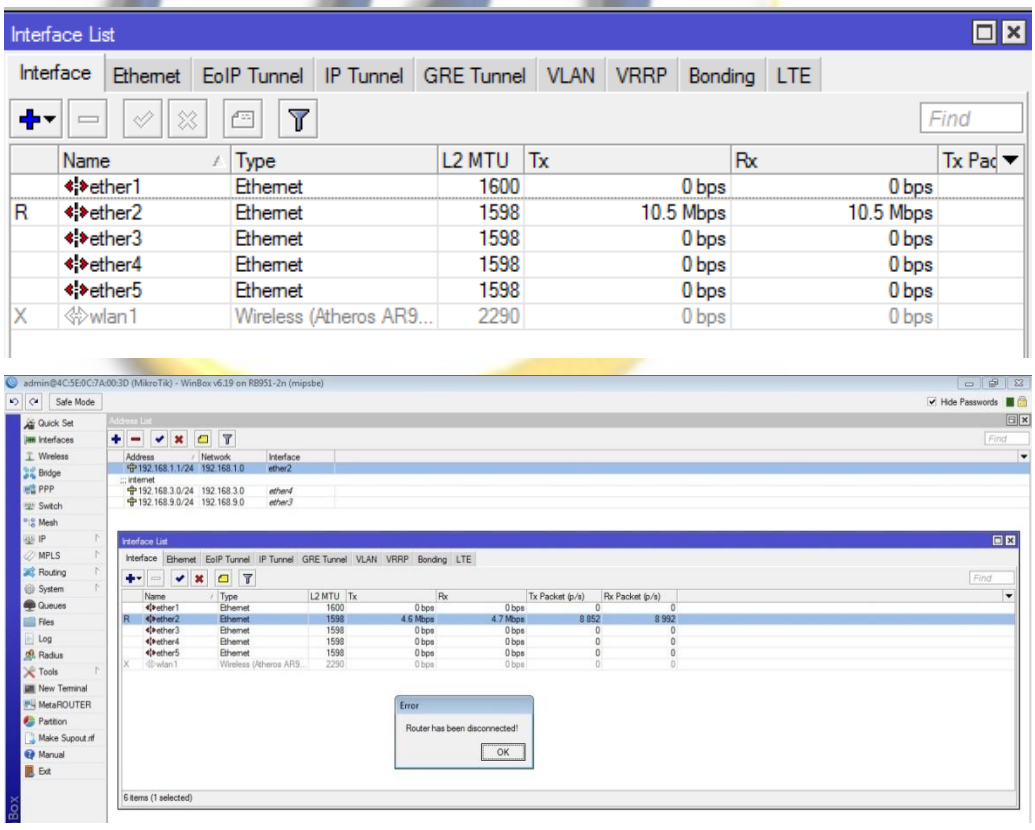
Namun *user* masih dapat membuka halaman website yang tidak ditentukan akan di blokir. Disini penulis mencoba membuka alamat halaman google dan web browser masih bisa mengakses halaman tersebut di jelaskan pada Gambar 4.35



Gambar 4.35 Tampilan Halaman Web Yang Tidak Terblokir

4.2.7 Pengujian Pengamanan Mikrotik Dari Serangan

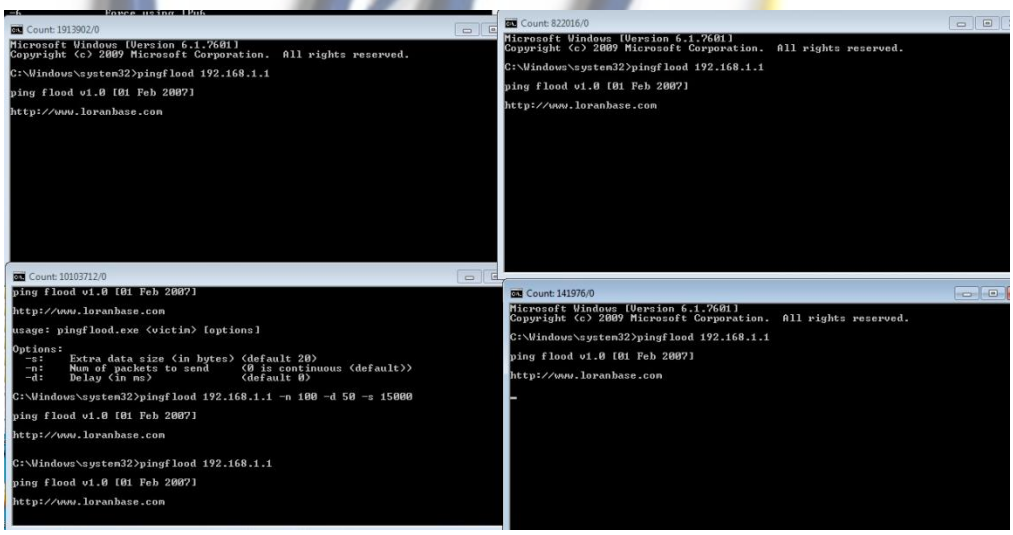
Salah satu serangan yang dilakukan oleh attacker atau hacker untuk melumpukan jaringan komputer adalah dengan melakukan serangan *Denial of Service Attack*. Dimana serangan ini akan membanjiri trafik sehingga komputer atau router akan menjadi terambil alih koneksinya kepada komputer yang melakukan serangan DoS sampai dimana proses dari komputer atau router meningkat dan bisa mengakibatkan komputer atau router menjadi *crash*. Akibatnya komputer atau router target bisa tidak dapat beroperasi di jelasakan pada Gambar 4.36 di bawah ini.



Gambar 4.36 Proses Router Mikrotik Down

Pada router MikroTik ini dapat melakukan penanganan dengan cara membatasi koneksi dengan batas koneksi yang diperbolehkan dari suatu alamat IP (*internet Protocol*).Jadi tiap koneksi yang diterima (*Incoming Connection*) akan dibatasi dalam melakukan koneksi sehingga tidak akan menyebabkan router mikrotik kehabisan *resource*.

Disini penulis melakukan pengujian DDOS dengan PingFlood**,** Software ini hanya dijalankan di Windows dan menggunakan *System* PING dan ICMP Protocol yang memungkinkan pengiriman paket dengan cepat. Korban yang terserang DSPF (sebut saja DoS *PingFlood*) akan mengalami peningkatan jaringan *Traffic* yang penuh dijelaskan pada Gmabar 4.37



Gambar 4.37 Proses DDos Pada Mikrotik dengan PingFlood

DoS Ping Flood adalah aplikasi yang dioperasikan pada sistem operasi windows. Buat yang belum mengetahui apa itu DDoS**.** *Pingflood* menggunakan metode *ping* dan mengunakan protokol ICMP, tetapi dalam paket dengan jumlah yang sangat banyak serta

sangat cepat pengirimannya. Ping flood dibuat oleh www.loranbase.com pada tanggan 1 Februari 2007. Versi yang saya share-kan saat ini adalah versi v1.0. Penggunaan ping flood harus pada sistem operasi windows karena aplikasi ping flood merupakan *executable* (berekstensi .exe) Korban dari ping flood ini antara lain modem, windows, Linux, router, dan *Server* . Semua sistem operasi dan mesin dijaringan komputer yang memiliki IP *Address* bisa diserang tanpa terkecuali. Efek dari *pingflood* ini, yaitu aktifitas komputer korban yang meningkat serta *traffic* jaringan komputer penuh.

Aplikasi ping sendiri aslinya digunakan untuk mengecek apakah sebuah host di jaringan komputer aktif atau tidak. Tetapi jika paket yang dikirim untuk ping jumlahnya terlalu banyak, maka hal ini dapat termasuk dalam katagori DDoS *Attack.*

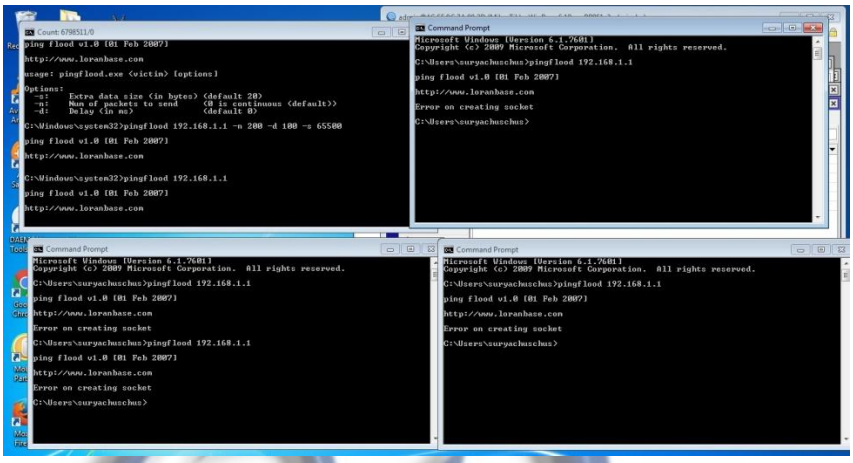
pingflood 192.168.1.3 -n 100 -d 50 -s 15000

Penjelasan :

- **pingflood**, artinya mengaktifkan aplikasi ping flood.
- **192.168.1.3**, adalah IP korban yang akan diserang menggunakan ping flood.
- **-n**, artinya jumlah paket yang berjumlah 100.
- **-d**, artinya delay tiap pengiriman paket.
- **-s 15000**, artinya ukuran data yang dikirim sebesar 15000 bytes.

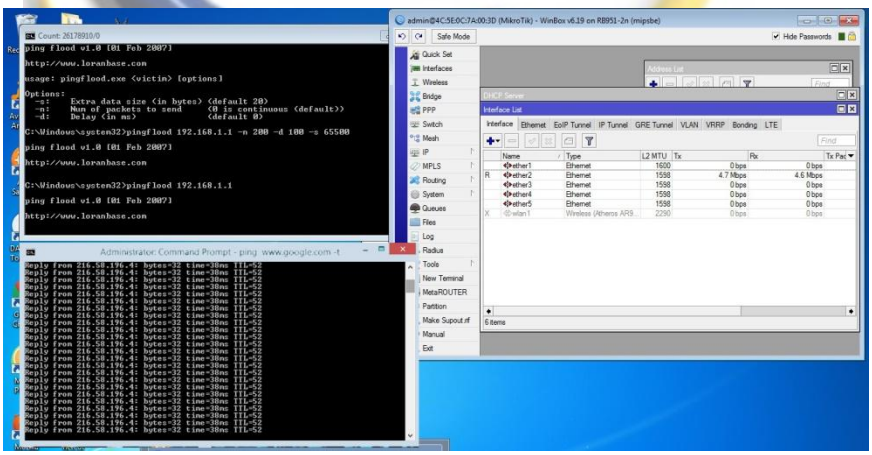
setelah membuat rull difirewall di mikrotik maka penulis melakukan uji coba kembali apakah rull yang telah dibuat tadi telah berjalan di mikrotik atau tidak berjalan dimikrotik. Dari hasil uji coba di

jelaskan pada Gambar 4.38 bahwa mikrotik memblok sehingga hanya dapat menjalankan 1 CMD *pingflood* pada PC.



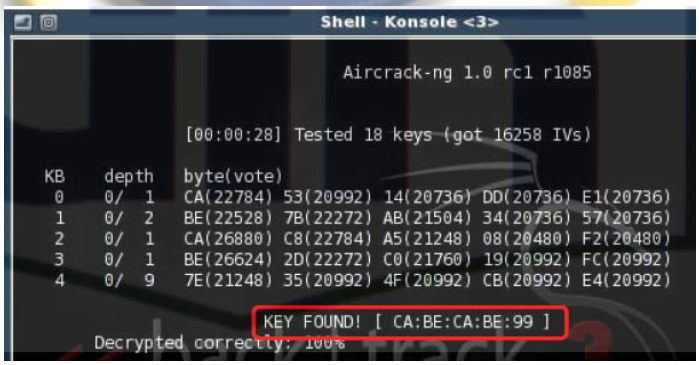
Gambar 4.38 Uji Coba Mikrotik Untuk di DDos

Dijelaskan pada Gambar 4.39 walau mikrotik dikirim paket data sebanyak Count 26178910 mikrotik tetap stabil dan internet tetap masih berjalan pada user



Gambar 4.39 Mikrotik Tetap Stabil Walau Telah di DDos

Mendapatkan WEP *key* yang digunakan oleh jaringan wireless bisa dikatakan impian dari setiap wireless hacker. Dengan mendapatkan WEP *key* ini, secara otomatis hacker telah mampu terhubung ke dalam jaringanwireless. Untuk pengguna rumahan yang menggunakan sebuah accesspoint sekaligus sebagai gateway ke Internet, artinya hacker akan mendapatkan akses Internet gratis secara ilegal WEP *Cracking* merupakan *Cracking* dengan metode statistik, karena itu untuk mendapatkan WEP *key*, dibutuhkan sejumlah data untuk dianalisa. Berapa banyak data yang dibutuhkan, tidak bisa ditentukan secara pasti, tergantung keberuntungan dan juga metode analisa yang digunakan. Tentu saja, semakin banyak data yang terkumpul, akan semakin memudahkan proses *Cracking* dalam mencari WEP *key*. Setelah mendapatkan data yang cukup banyak, seorang hacker tinggal menjalankan program *Cracking* yang akan menganalisa data-data yang telah terkumpul untuk mendapatkan WEP *key*. Berapa lama proses *Cracking* ini akan sangat tergantung kepada kecepatan komputer yang digunakan, jumlah data yang tersedia dan jumlah karakter yang digunakan oleh WEP *key* tersebut.

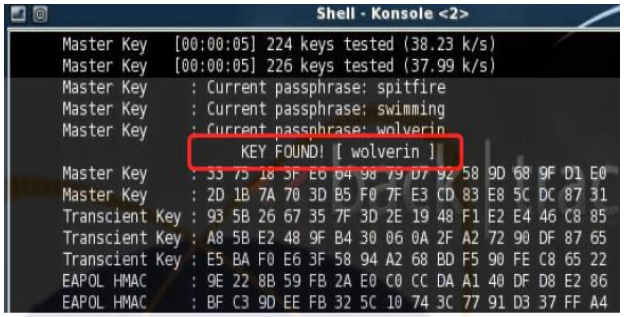


Gambar 4.40 Proses WEP *Cracking*

Tahapan untuk mendapatkan *key* dari sebuah jaringan WPA/WPA2 sebagai berikut :

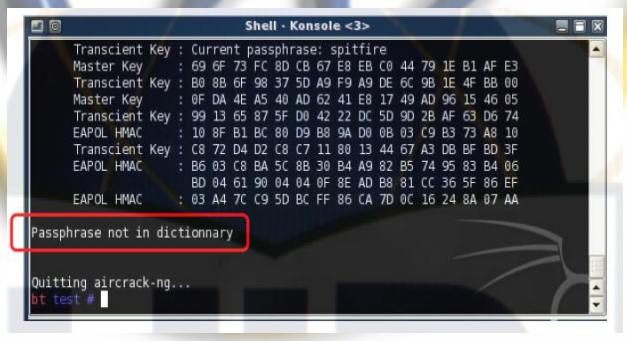
1. Mencari infomarsi jaringan wireless yang hendak dihack.

2. Mendapatkan paket handshake
3. Melakukan crack WPA/WPA 2 dengan *dictionary file*



Gambar 4.41 Proses WPA 2 *Cracking*

Pada radius server untuk mendapatkan paket data handshake cukup sulit dan sering mengalami kegagalan dan bila berhasil mendapat paket handshake proses *Cracking* password tidak mampul di tembus



Gambar 4.42 Aircrack Gagal Menemukan Password

Tabel 4.4 Perbandingan Keamanan Radius Sever

Jenis Serangan	**Tanpa Radius Server**	**Penerapan Radius Server**
Denial Of servise	Berhasil	Gagal
Mac Clon	Berhasil	Gagal

Net Cut	Berhasil	Gagal
Aircrack	Berhasil	Gagal

Dari Hasil Pengujian keamanan pada tahapan ini :

- Hidden SSID tidak bisa diterapkan sebagai sebuah teknik keamanan karena pada dasarnya itu hanya menyembunyikan SSID dari user biasa
- Mac Filtering yang dianggap mampu memfilter user berdasarkan MAC Address pun tidak bisa diandalkan, sebab Mac Address dapat diubah dengan mudah secara virtual
- Enkripsi WEP memiliki banyak kelemahan yang sangat rentan, sehingga dapat dijebol
- Walaupun keamanan WPA/WPA2 menggunakan enkripsi AES yang cukup kuat saat ini, namun masih memungkinkan untuk dijebol bila menggunakan passphare yang lemah