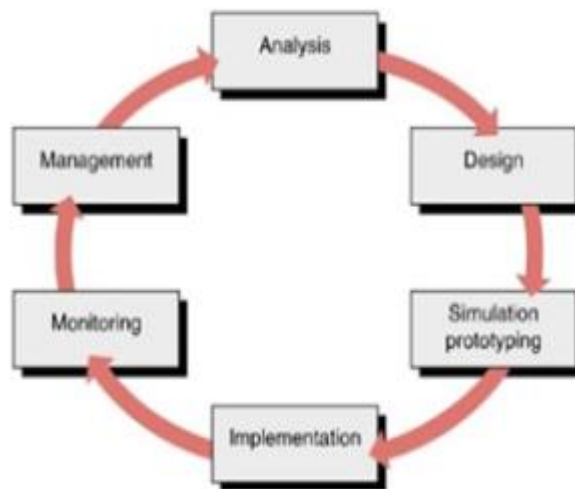


BAB III

METODOLOGI PENELITIAN

1. METODE PENDEKATAN MASALAH

Metode pendekatan yang digunakan dalam penelitian ini adalah metode NDLC (*Network Development Life Cycle*). NDLC sendiri memiliki beberapa tahap diantaranya adalah analisis, desain, simulasi, implementasi, pemantauan, dan manajemen.



Gambar 3. 1 siklus NDLC

1. Analisis

Tahap analisis disini penulis menganalisis sistem keamanan yang ada pada jaringan di Cafe Rodeo. Penulis melakukan pengecekan terhadap jaringan dengan cara melakukan percobaan scanning ip dan scanning port untuk mengetahui apakah ada celah terhadap jaringan atau tidak. Ternyata scanning dapat dilakukan sehingga penulis tau bahwa jaringan tersebut memiliki celah yang berpotensi mengalami penyadapan ataupun penyusupan. Karena dengan data yang diperoleh dari hasil scanning yang berupa informasi-informasi baik berupa IP address , port yang aktif dan penemuan akun serta passwordnya dapat dijadikan bekal untuk menyadap data.

2. Desain

Setelah mengetahui apa yang akan dijadikan acuan dari penelitian penulis akan mendesain bagaimana sistem yang akan diterapkan pada jaringan untuk mengoptimalkan keamanan jaringan di Cafe Rodeo. Penulis akan menggunakan metode Access Control List (ACL) untuk dapat mengatur akses pada jaringan. Lalu lintas akses data agar lebih terorganisir oleh admin, sehingga admin dapat menentukan apa saja yang boleh diakses oleh user dan apa saja yang tidak boleh diakses oleh user. Jika admin tidak menghendaki user mengakses suatu website maka admin akan memblokir akses terhadap website tersebut. pada tahap ini penulis menyiapkan segala sesuatu yang dibutuhkan dalam merancang manajemen dan sitem keamanan untuk Café Rodeo.

3. Simulasi

Setelah penulis mendesain rancangannya maka penulis akan mensimulasikan hasil rancangannya terhadap jaringan di Café tersebut. Penulis melakukan ujicoba terhadap rancangannya untuk mengetahui keberhasilan dari rancangannya tersebut. setelah ujicoba dilakukan penulis melakukan evaluasi terhadap rancangan sistem untuk mengoptimalkan hasil rancangan sebelum benar-benar diimplementasikan pada jaringan.

4. Implementasi

Penulis akan menerapkan hasil rancangannya pada jaringan di café agar jaringan di cefe lebih gampang di pantau manajemen aksesnya.

5. Pemantauan

Jika rancangan sudah di terapkan pada jaringan cafe, admin akan memantau perkembangan dari sistem yang telah diterapkan. Selama masa pemantauan admin akan lebih memahami cara penggunaan dan perawatan sistem yang lebih baik dan sesuai dengan jaringan.

6. Manajemen

Setelah melewati semua tahapan disini penulis akan lebih mudah menentukan metode apa yang ingin digunakan untuk memanajemen sistem kedepannya.

Setelah manajemen tahap pertama telah dilakukan dan mengetahui hasil dari pantauan, penulis akan lebih mudah memajemen apa saja yang akan dilakukan untuk menghadapi situasi yang terjadi nantinya.

2. LATAR PENELITIAN

Penelitian ini dilakukan untuk mengetahui proses pengembangan atau pembuatan desain keamanan jaringan dengan mendeskripsikan hasil temuan penelitian. Pendekatan yang digunakan pada saat penelitian adalah pendekatan kualitatif, mengapa demikian karena dengan metode ini data yang ada dilapangan dapat terungkap dan diuraikan serta menginterpretasikan data yang apa adanya sesuai data di lapangan, dan menghubungkan sebab akibat terhadap sesuatu yang terjadi pada saat penelitian dengan tujuan memperoleh gambaran realita mengenai kelemahan keamanan jaringan yang ada. Objek penelitian dilakukan di Cafe Rodeo Blora. Dimana permasalahan yang diambil atau dihadapi dalam penelitian ini yaitu sistem pada keamanan jaringan yang diterapkan pada Cafe Rodeo masih belum optimal.

Tidak adanya pengontrol atau pengelola keamanan yang dapat mengidentifikasi pihak atau seseorang yang dapat mengakses atau menggunakan jaringan wireless secara percuma dalam hal ijin akses dan monitoring data sehingga banyak sekali kesalahan atau pelanggaran yang dilakukan baik dari dalam (para staff bekerja cafe dan pembeli) atau luar cafe (pihak yang berdekatan dengan lokasi cafe sehingga bisa setiap kali membobol atau menghacker layanan jaringan yang ada). Dari kelemahan yang ada pada sistem

jaringan tersebut akan timbul beberapa permasalahan lainnya di antaranya ketika ada banyak user yang mengakses jaringan tersebut maka internet akan terasa lambat ditambah dengan pengguna yang menghacker jaringan tersebut bisa melakukan hal-hal yang mungkin tidak akan diketahui oleh pemilik cafe tersebut. Disisi lain juga pemilik cafe akan merasa dirugikan dalam hal biaya dan lain-lain karena pemakaian akses internet yang secara gratis didapatkan oleh pihak yang tidak berwenang tersebut. Informan yang digunakan adalah seorang karyawan di Cafe Rodeo.

3. FOKUS PENELITIAN

Objek dalam penelitian adalah sistem keamanan jaringan. Menurut Moh Nazir (2005) adanya Identifikasi variabel perlu dilakukan setelah peneliti merumuskan segala sesuatunya yang mendukung keputusan akhir mulai dari masalah penelitian, lalu keputusan apa yang akan di ambil untuk menindaklanjuti permasalahan kemudian merumuskan hipotesis, karena dengan konsep yang jelas dan konsep yang sudah diubah bentuknya variabel dapat diukur dan digunakan secara operasional. Dalam penelitian ini variabel dapat dipecahkan ke dalam dua variabel yaitu variabel terikat (dependent) dan variabel bebas (independent):

1. Variabel Bebas (Independent)

Variabel bebas atau independent dalam penelitian ini yaitu akibat dari lemahnya keamanan jaringan yang dapat berpotensi mengalami kerusakan data ataupun penyalahgunaan hak akses oleh pihak yang tidak berwenang.

2. Variabel Terikat (Dependent)

Varibel terikat (dependent) dalam penelitian ini yaitu Sistem Keamanan Jaringan Menggunakan *Access Control List* untuk Cafe Rodeo.

4. SUMBER DATA

Untuk pengumpulan data dilakukan secara langsung pada sumbernya maupun pengumpulan data secara tidak langsung. Untuk metode pengumpulan data yang dilakukan adalah sebagai berikut:

1. Data primer

Data primer disini diperoleh langsung dari sumber data di Cafe Rodeo. Penulis melakukan wawancara dengan karyawan café rodeo dan penulis melakukan percobaan pada objek.

2. Data sekunder

Data sekunder disini diperoleh dari pengumpulan data dari buku-buku ataupun jurnal baik nasional maupun internasional mengenai sistem keamanan jaringan ACL yang memiliki kemiripan dalam pembuatan perancangan sistem keamanan jaringan hal ini sebagai tambahan atau support data dari data yang berhubungan dengan objek yang akan menjadi penelitian.

5. TEKNIK PENGUMPULAN DATA

Untuk metode pengumpulan data yang digunakan meliputi:

1. Interview

Metode yang dilakukan dengan cara tanya jawab secara langsung dengan sumber data atau secara tatap muka seperti bimbingan dan konseling dengan staff pekerja.

Wawancara yang dilakukan ini bertujuan untuk mendapatkan informasi yang lengkap.

2. Studi literature

Studi literatur adalah salah satu metode pengumpulan data dengan cara membaca buku dan jurnal sesuai dengan data yang dibutuhkan. Pada penelitian ini penulis memilih studi literatur untuk mengumpulkan referensi dari jurnal dan beberapa artikel tentang jaringan dan mengenai sistem keamanan jaringan khususnya sistem keamanan dengan metode ACL (Access Control List) serta jurnal yang memiliki kemiripan dalam pembuatan perancangan sistem keamanan jaringan.

3. Observasi

Suatu teknik yang dilakukan dengan cara pengumpulan data secara cermat dan sistematis terhadap prosedur yang ada serta mencatat apa saja hasil dari data yang dikumpulkan. Penulis melakukan observasi dengan cara mendatangi langsung tempat yang akan menjadi objek penelitian yaitu jaringan yang ada pada Café Rodeo dan mencari tahu apa saja kendala jaringan yang dialami sehingga penulis dapat mengetahui apa saja yang akan diperlukan untuk pengoptimalan sistem serta peningkatan keamanan jaringan

yang dimiliki. Metode ini akan memberikan gambaran awal tentang pengelolaan jaringan di Cafe Rodeo.

6. TEKNIK KEABSAHAN DATA

Penulis akan melakukan suatu analisis dalam penelitian ini agar mengetahui bagaimana kondisi sistem keamanan jaringan yang sebelumnya. Pada penelitian ini penulis melakukan beberapa *scanning* dan *sniffing* untuk mengetahui kondisi jaringan pada Café Rodeo. Dengan melakukan *scanning* dan *sniffing* penulis menarik rumusan permasalahan terhadap sistem keamanan pada jaringan tersebut.

Setelah penulis menganalisis permasalahan yang ada maka penulis akan mencari jalan keluar untuk masalah tersebut dan mengujicobanya terlebih dahulu sebelum mengimplementasikan sistem keamanan yang baru pada jaringan yang ada. Jalan keluar yang diambil oleh penulis pada penelitian ini yaitu dengan cara merancang manajemen akses dan sistem keamanan pada jaringan agar akses dapat di kendalikan dan keamanan lebih optimal. Pada penelitian ini penulis menggunakan metode access control list (ACL) untuk merancang sistem keamanan yang akan digunakan pada jaringan di Café Rodeo. Penulis akan mendesain bagaimana proses pembuatan, cara kerja sampai cara perawatan sistem keamanan yang akan digunakan. Desain yang dirancang tidak akan langsung diterapkan pada jaringan melainkan harus dilakukan uji coba dahulu untuk mengetahui kemampuan dan kualitas sistem keamanan itu sendiri. Hasil dari uji coba tersebut akan dievaluasi terlebih dahulu agar kinerja lebih

optimal dan jika sudah benar-benar maksimal sesuai dengan harapan dan tidak ada masalah maka sistem bisa diterapkan pada objek.

Jika rancangan yang dibuat sudah diterapkan maka akan dipantau bagaimana kinerjanya dan keoptimalannya dalam mefilter paket data dan menejemen aksesnya terhadap jaringan. Setelah terkondisi sesuai harapan maka perawatan terhadap sistem akan dilakukan oleh admin agar kerja sistem tetap optimal.

7. TEKNIK ANALISIS DATA

Dalam penelitian ini, penulis menganalisis menggunakan metode kualitatif kerana peneliti mengumpulkan data dengan cara bertatap muka atau wawancara serta melakukan survey langsung kelapangan. Adapun yang akan menjadi pedoman dalam mengumpulkan data dalam tahap analisis ini adalah jumlah *user* dan kegiatan yang sering dilakukan, peralatan yang ada, data yang dapat diakses dari peralatan, status jaringan, jumlah pelanggan serta sistem keamanan yang sudah ada.

1. Tempat Dan Waktu Penelitian

Penelitian dilakukan di Rodeo Angkring & Café yang terletak di Jl. Donorejo Sawah No.1, Desa Jejeruk Kecamatan Blora, Kabupaten Blora, Jawa Tengah. Waktu yang dibutuhkan oleh penulis untuk melakukan penelitian adalah 3 bulan terhitung dari bulan November sampai bulan Januari.

2. Alat Penelitian

Tabel 3. 1 Alat dan Bahan Untuk Penelitian

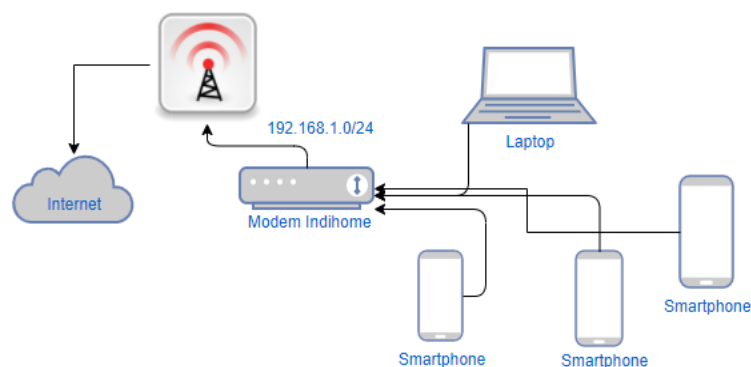
HARDWARE	SOFTWARE
Pc/Laptop	Anggry Ip Scanner
Mikrotik RB941-2 nD	Nmap-Zenmap
Kabel Utp	Wireshark
Modem Wifi/Acces Point	Winbox
	Kapasitas bandwith 10 mbps

3. Analisis Perancangan Sistem Di Cafe Rodeo

a) Analisis sistem yang sedang berjalan

Berdasarkan dari analisis penelitian yang telah dilakukan di lapangan secara keseluruhan, sistem keamanan jaringan pada cafe tersebut masih mempunyai kendala, Dimana permasalahan yang diambil atau dihadapi dalam penelitian ini yaitu sistem pada keamanan jaringan yang diterapkan

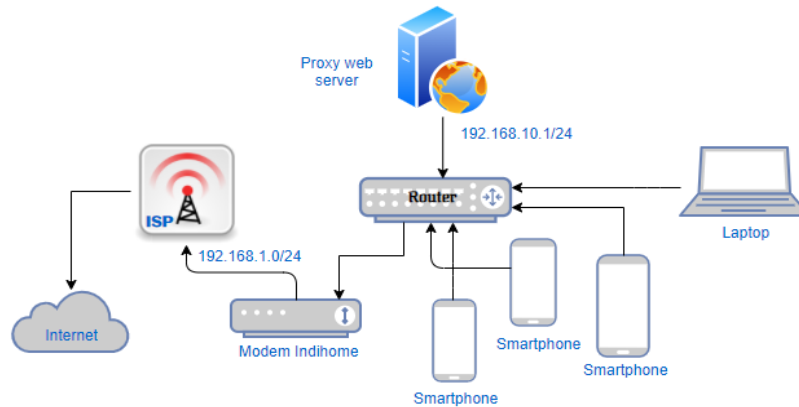
pada Cafe Rodeo masih belum optimal. Tidak adanya pengontrol atau pengelola keamanan yang dapat mengidentifikasi pihak atau seseorang yang dapat mengakses atau menggunakan jaringan wireless secara percuma dalam hal ijin akses dan monitoring data sehingga banyak sekali kesalahan atau pelanggaran yang dilakukan baik dari dalam (para staff bekerja cafe dan pembeli) atau luar cafe (pihak yang berdekatan dengan lokasi cafe sehingga bisa setiap kali membobol atau menghacker layanan jaringan yang ada). Berikut topologi sistem jaringan yang sedang berjalan dapat dijelaskan sebagai berikut:



Gambar 3. 2 Jaringan Awal Pada Café Rodeo

Pada gambar topologi jaringan tersebut bisa digambarkan bahwa akses client pada jaringan dapat dilakukan secara langsung pada modem isp untuk melakukan koneksi pada internet atau wifi. Secara tidak langsung dan tidak disadari ini dapat menimbulkan client bisa mengatur akses terhadap modem dengan mengetahui network yang dipakai pada isp ketika client terhubung pada jaringan.

b) Analisis sistem yang diusulkan



Gambar 3. 3 Topologi Jaringan Yang Dibuat

Alat yang digunakan dalam percobaan adalah sebagai berikut :

- 1) Modem ISP yang digunakan untuk penghubung antara mikrotik dan untuk membuat bridge
- 2) Mikrotik digunakan untuk mengatur keseluruhan sistem keamanan
- 3) Kabel UTP digunakan untuk menghubungkan wifi pada router dan PC atau laptop pada mikrotik. Berikut ini adalah IP yang akan dimasukkan pada port mikrotik dan modem untuk menghubungkan jaringan dan membuat sistem baru:
 - a) Pada port LAN1 yang terdapat pada modem wifi dihubungkan menggunakan kabel pada mikrotik ether1 supaya terdapat dan terhubung pada koneksi internet yang ada pada modem wifi.

b) Pada port mikrotik ether2 dihubungkan menggunakan kabel pada PC atau laptop untuk mengatur IP yang akan dibagikan pada Client nantinya

4) Setting IP tersebut diantaranya:

a) Wifi ke mikrotik : menggunakan alamat Ip Address (192.168.1.12/24) dan menggunakan Network atau Koneksi internet pada Modem Wifi (192.168.1.0) pada ether1.

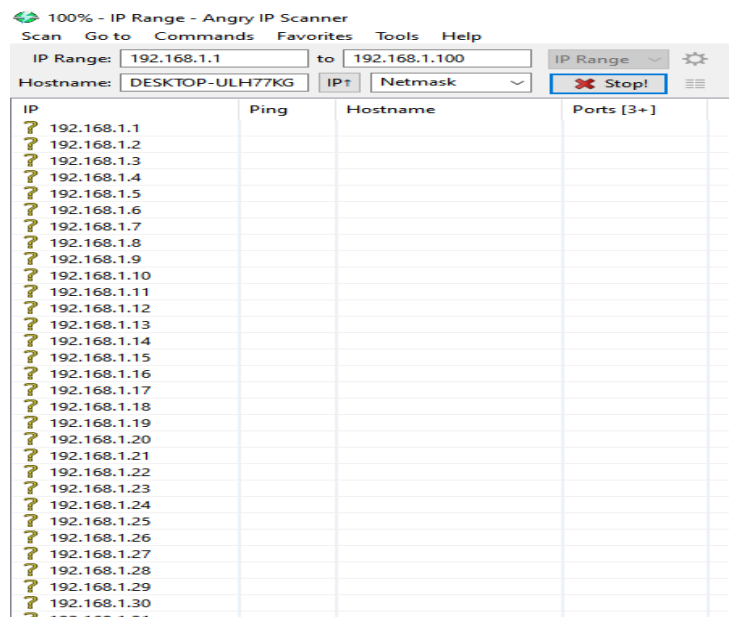
b) Mikrotik ke Pc: menggunakan alamat Ip Address (192.168.10.1/24) dan menggunakan Network atau Koneksi internet ke mikrotik (192.168.10.0) pada ether2.\

/24 digunakan karena jaringan wifi memiliki satu pusat jaringan atau satu router yang mana nanti dapat digunakan oleh banak pengguna ddi lingkup jaringan.

5) Aplikasi Winbox untuk masuk pada pengaturan Mikrotik.

4. Percobaan penyerangan pada jaringan Cafe Rodeo

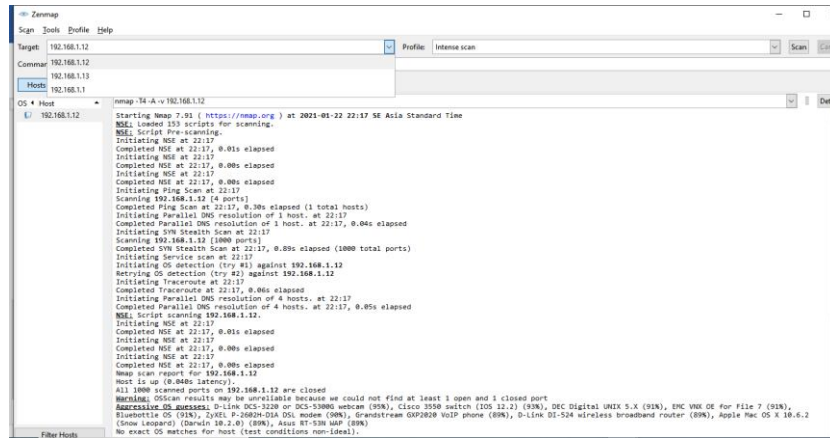
a. Percobaan Scanning Ip



Gambar 3. 4 Proses Scanning Ip

Scanning ip dilakukan dengan menggunakan software ip scanner. Aplikasi ini dapat memberikan informasi terkait ip address yang terdeteksi pada jaringan. Aplikasi ini dapat memunculkan data Ip yang sedang aktif pada jaringan. Percobaan scanning ip ini dilakukan dengan range ip 192.168.1.1 sampai 192.168.1.100.

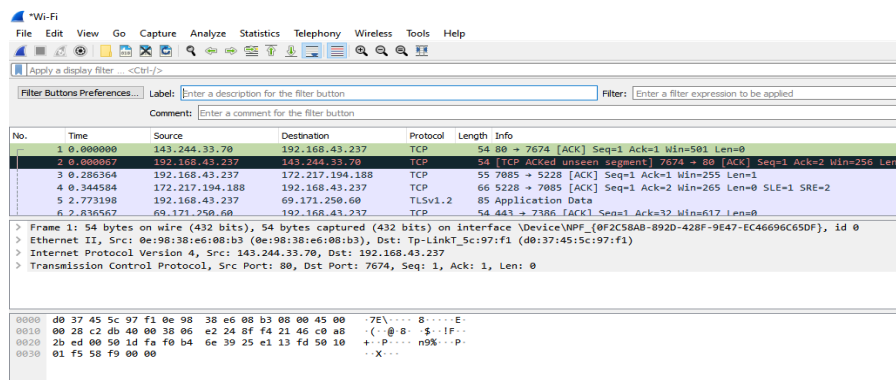
b. Percobaan Scanning Port



Gambar 3. 5 Proses Scanning Port

Scanning port dilakukan dengan menggunakan aplikasi Nmap-Zenmap. Aplikasi ini dapat memberikan informasi terkait port-port yang terbuka dan bebas diakses pada suatu jaringan. Dengan aplikasi ini penulis dapat memilih ip address yang ingin di pilih untuk mengetahui informasi terkait port-port yang terbuka dan tidak terbuka.

c. Percobaan Sniffing



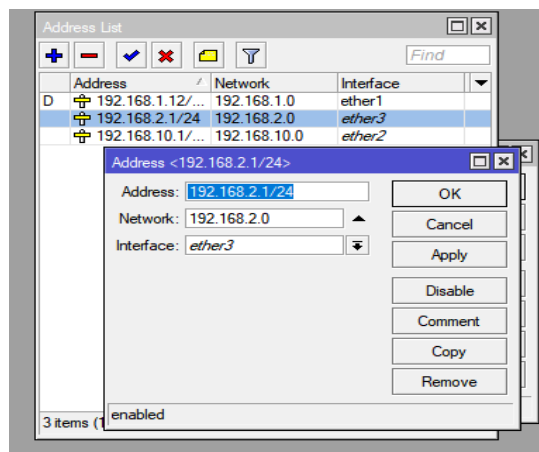
Gambar 3. 6 Proses Percobaan Sniffing

Percobaan *sniffing* dilakukan menggunakan aplikasi wireshark. Aplikasi ini dapat membantu kita untuk memperoleh informasi berupa akun dan password korban yang menjadi korban *sniffing*. Namun informasi yang diperoleh hanya akun yang melewati jaringan yang sedang dimonitoring. Dalam suatu jaringan pasti ada beberapa Ip Address yang sedang terhubung di dalamnya dan dapat dipilih salah satu Ip Address untuk dilakukan percobaan *sniffing* untuk mengetahui informasi di dalamnya.

5. Perancangan Manajemen Akses Dan Sistem Keamanan

a. Setting Ip Address

Setting Ip adalah Langkah awal dalam merancang sistem jaringan ini.

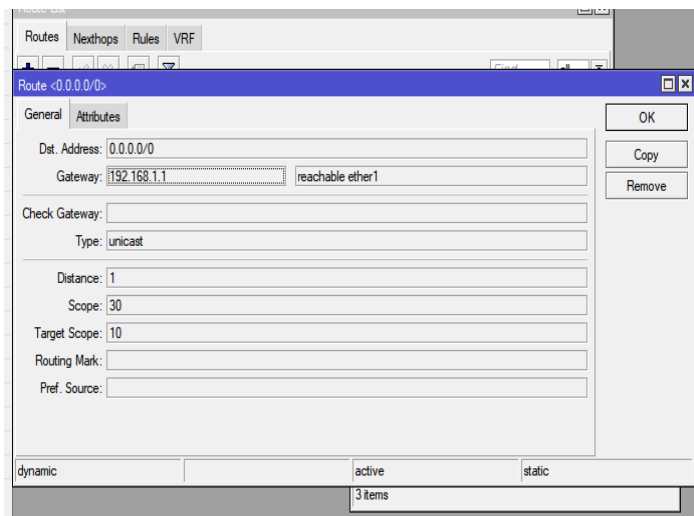


Gambar 3. 7 Proses Setting Ip Address

Setting ini dilakukan pada aplikasi winbox dimana di dalamnya menyediakan banyak menu yang data menyeting berbagai aspek dalam

jaringan. Untuk setting ip address penulis menggunakan ip IP Address (192.168.1.12 pada ether1) dan (192.168.10.1 pada ether2)

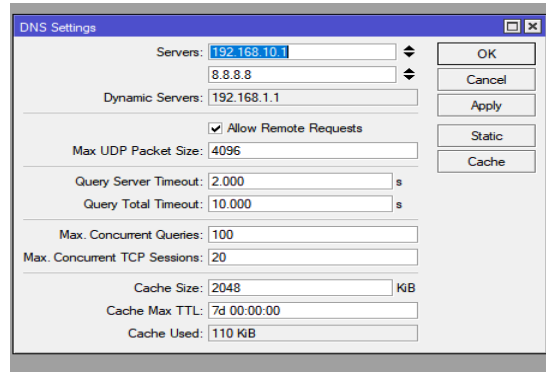
b. Gateway



Gambar 3. 8 Setting Gateway

Setting gateway dilakukan pada menu ip dengan memasukkan alamat gateway dan mengosongi address nya atau membiarkanya dengan 0.0.0.0/0.

c. DNS



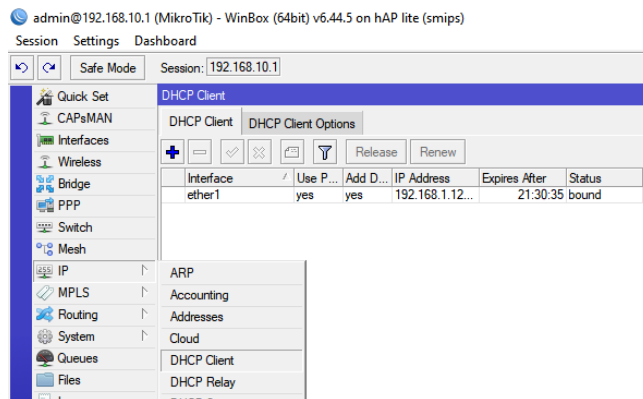
Gambar 3. 9 Setting DNS

Setting Domain Name System ini dilakukan pada setting Ip lalu pada menu DNS. Setting ini memiliki tujuan agar internet dapat berjalan.

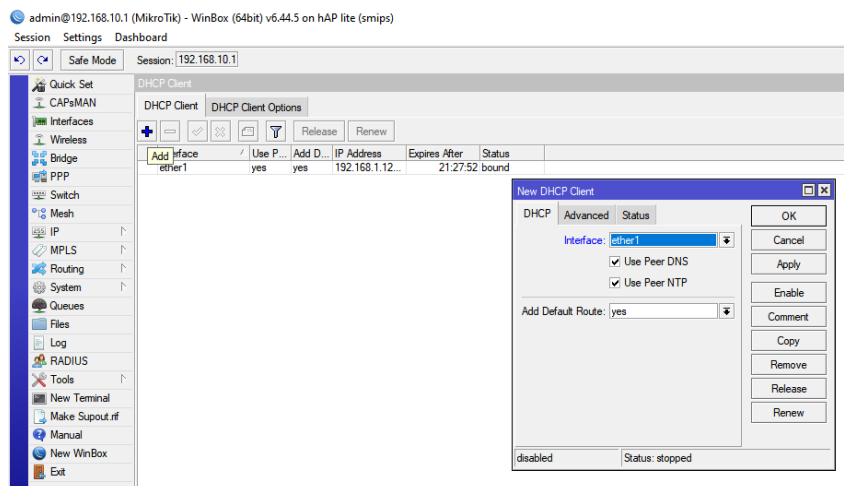
d. Setting DHCP

1. Settings Dhcp Client

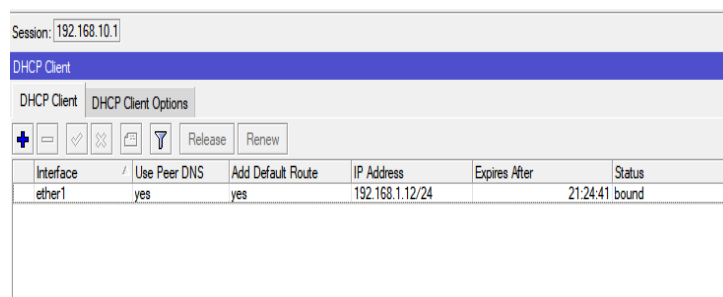
Masuk pada pengaturan DHCP Client terdapat pada menu IP lalu DHCP client klik tanda + kemudian pilih interface/ether yang mengarah ke internet atau ke modem ISP terus OK. Penulis disini menggunakan Ether1 untuk menghubungkan Mikrotik pada Modem Isp atau WIFI



Gambar 3. 10 Tampilan Menu DHCP Client Terdapat Pada Menu IP



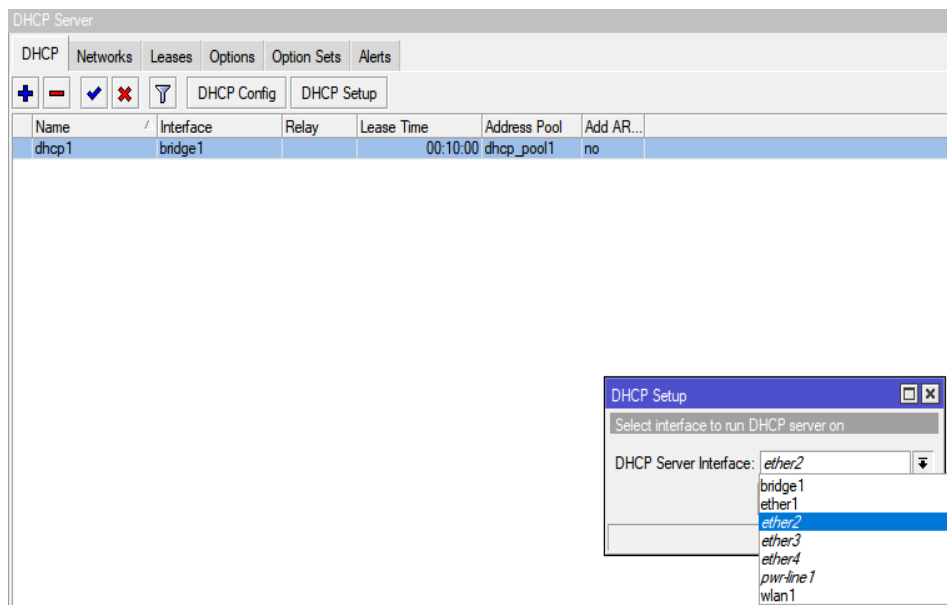
Gambar 3. 11 Tampilan menu tambah DHCP Client



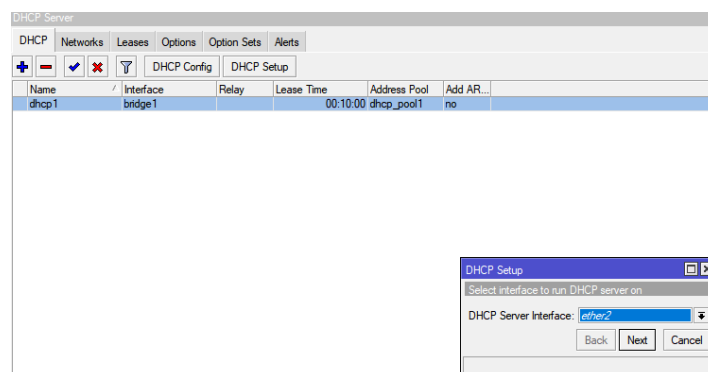
Gambar 3. 12 Tampilan Setting DHCP Client

2. Settings Dhcp Server

Pada DHCP setup, masuk pada menu pengaturan IP lalu klik dhcp setup kemudian pilih interface yang menuju ke lokal atau Lan (ether2 yang digunakan penulis untuk ke lokal) dan next next sampai selesai, bila sudah maka tampilan akan terlihat seperti dibawah ini tetapi penulis disini akan membuat suatu bridge agar setiap client dapat berbagi data atau file-file penting menggunakan satu jaringan.



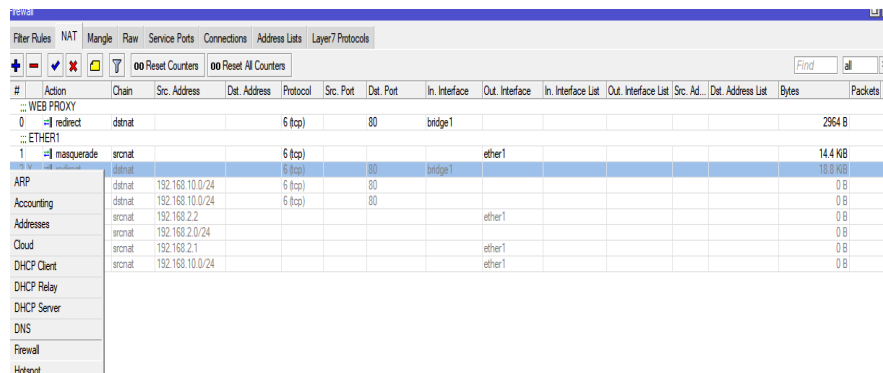
Gambar 3. 13 Tampilan Pilihan DHCP Setup Ether2 Pada IP DHCP Server



Gambar 3. 14 Membuat Ether2 Dan Tampilan Bridge1 Pada IP DHCP Server

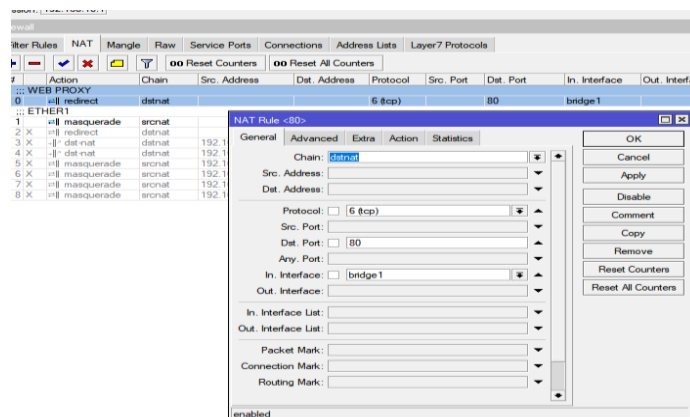
e. NAT

Pada menu IP pilih Firewall lalu pilih nat klik tanda + kemudian chain = dstnat protocol = tcp dst. ports = 80 in-interface = interface/ether yang ke wifi lokal(bridge1) action= redirect to ports=8080 untuk web proxy dan nantinya akan diakses client, sedangkan pada ether1 pilih atau buat chain = srcnat protocol = tcp out-interface= interface/ether yang ke internet(ether1) action=masquarade.

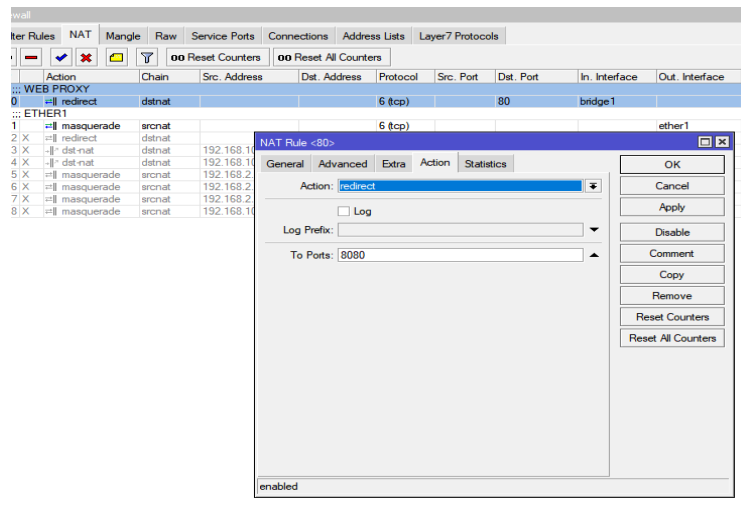


#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Src. Ad...	Dst. Address List	Bytes	Packets
WEB PROXY															
0	redirect	dstnat			6 (tcp)		80	bridge1						2964 B	
ETHER1															
1	masquerade	srcnat			6 (tcp)				ether1					14.4 KB	
ETHER1															
	dstnat				6 (tcp)		80	bridge1						18.8 KB	
2	dstnat		192.168.10.0/24		6 (tcp)		80							0 B	
3	dstnat		192.168.10.0/24		6 (tcp)		80							0 B	
4	srcnat		192.168.2.2						ether1					0 B	
5	srcnat		192.168.2.0/24						ether1					0 B	
6	srcnat		192.168.2.1						ether1					0 B	
7	srcnat		192.168.10.0/24						ether1					0 B	

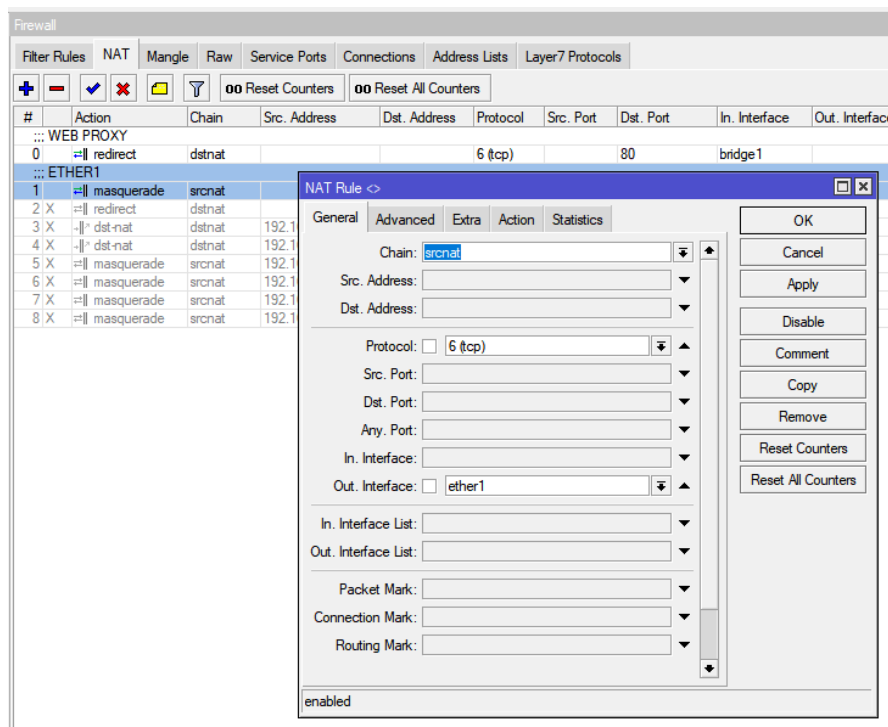
Gambar 3. 15 Tampilan Menu Ip Firewall Nat



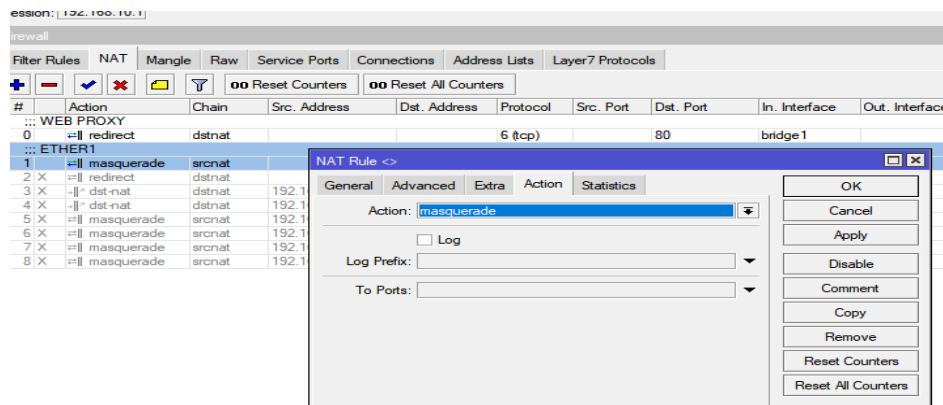
Gambar 3. 16 Tampilan Setting Ip Firewall Nat Untuk Web Proxy Pada Tab General



Gambar 3. 17 Tampilan Setting Ip Firewall Nat Untuk Web Proxy Pada Tab Action



Gambar 3. 18 Tampilan Setting Ip Firewall Nat Untuk Ether1 Pada Tab General



Gambar 3. 19 Tampilan Setting Ip Firewall Nat Untuk Web Proxy Pada Tab Action

#	Add	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Src. Ad...	Dst. Address List	Bytes	Packets
WEB PROXY																
0		=> redirect	dstnat			6 (tcp)		80	bridge1							2964 B
ETHER1																
1		=> masquerade	srcnat			6 (tcp)				ether1						145 KB
2	X	=> redirect	dstnat			6 (tcp)		80	bridge1							18.8 KB
3	X	=> dst-nat	dstnat	192.168.10.0/24		6 (tcp)		80								0 B
4	X	=> dst-nat	dstnat	192.168.10.0/24		6 (tcp)		80								0 B
5	X	=> masquerade	srcnat	192.168.2.2						ether1						0 B
6	X	=> masquerade	srcnat	192.168.2.0/24												0 B
7	X	=> masquerade	srcnat	192.168.2.1						ether1						0 B
8	X	=> masquerade	srcnat	192.168.10.0/24						ether1						0 B

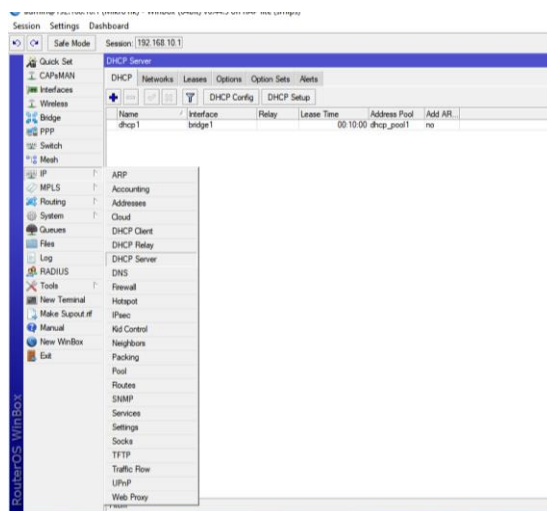
Gambar 3. 20 Tampilan Ip Firewall Nat Keseluruhan

f. Setting Bridge atau setting terhubung pada wifi lokal

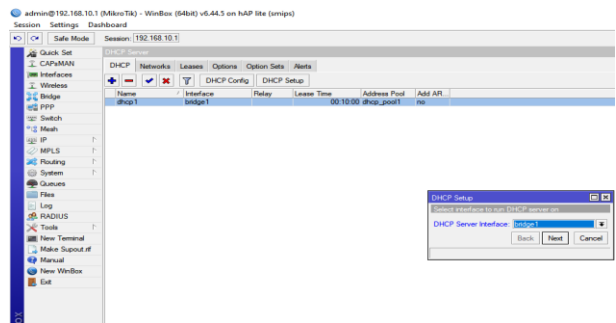
1. Setting Bridge pada DHCP Server

Karena penulis disini akan membuat suatu wifi yang akan terhubung pada beberapa Client Lokal dan tidak mempunyai suatu alat Switch Hub untuk menghubungkan beberapa client yang banyak maka penulis akan membuat suatu metode Bridge atau bridging. Teknik Bridging

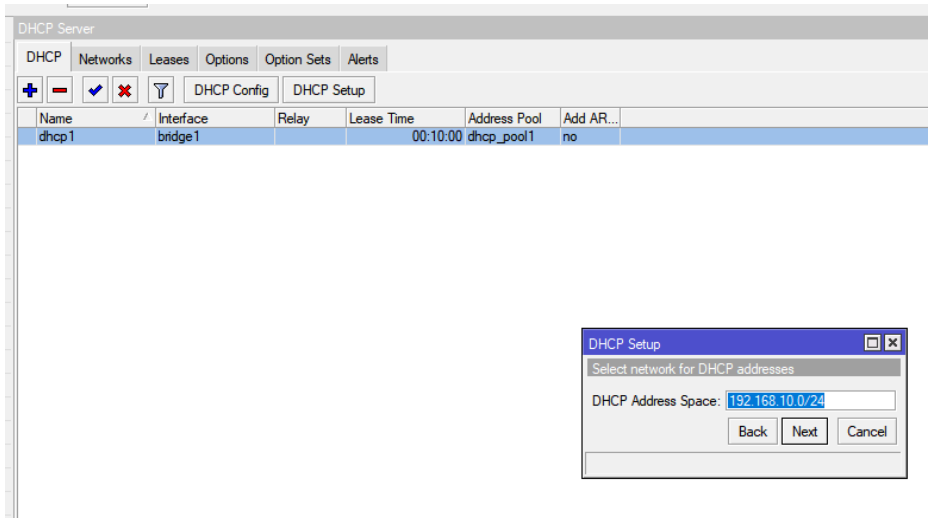
juga bisa digunakan untuk memonitoring trafik antar port. Jika sebelumnya sudah membuat dhcp setup yang ada pada IP DHCP Server di ether2 yang dibuat untuk client maka itu akan diubah dan diganti menjadi (bridge1) untuk wifi lokal dan koneksi antar client , dan selanjutnya untuk membuat atau melakukan Brigging mikrotik tersebut dapat dilakukan dengan cara Pilih menu Bridge pada winbox lalu buat bridge baru dengan klik tanda (+) dan berikan nama sesuai dengan yang diinginkan jika sudah klik Ok. Selanjutnya, Pada Tab yang ada Pada menu Bridge pilih Port lalu klik + dan masukkan wlan1 dan ether2 pada interface dan bridge pilih nama Bridge yang tadi sudah dibuat sebelumnya. Penulis memberikan nama pada Bridge (Bridge1). Dimana wlan1 adalah untuk sumber internet pada wifi lokal dan ether 2 adalah untuk client akses pada wifi lokal dan nantinya (wlan1 dan Ether2) akan menjadi bridge untuk wifi lokal.



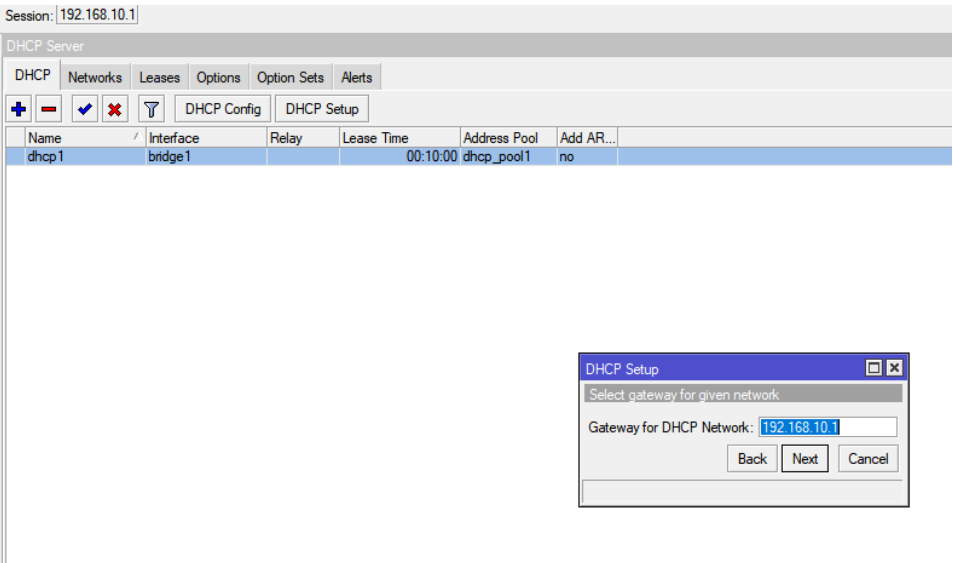
Gambar 3. 21 Tampilan Pengaturan Dhcp Server Pada Menu IP



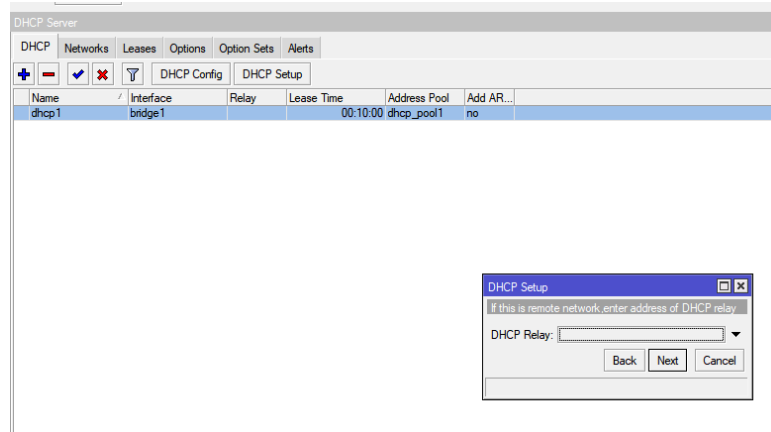
Gambar 3. 22 Tampilan Dhcp Setup Bridge1 Next1



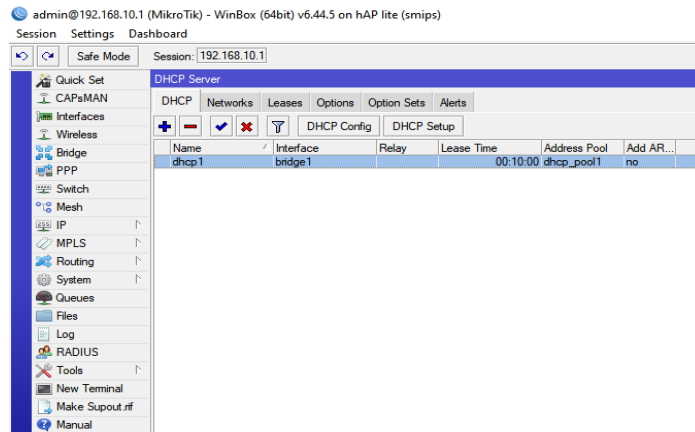
Gambar 3. 23 Tampilan DHCP Setup Bridge Next3



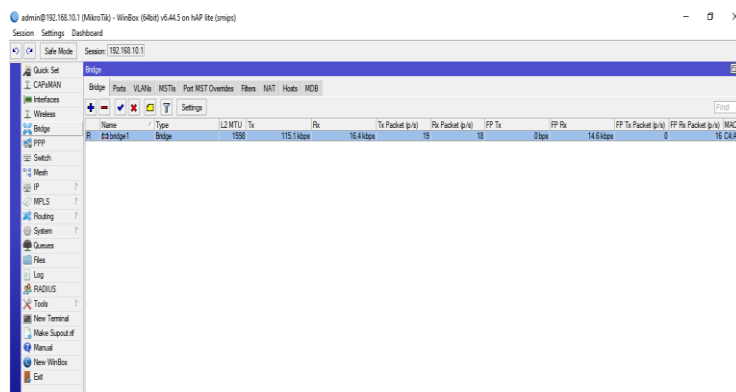
Gambar 3. 24 Tampilan DHCP Setup Bridge Next4



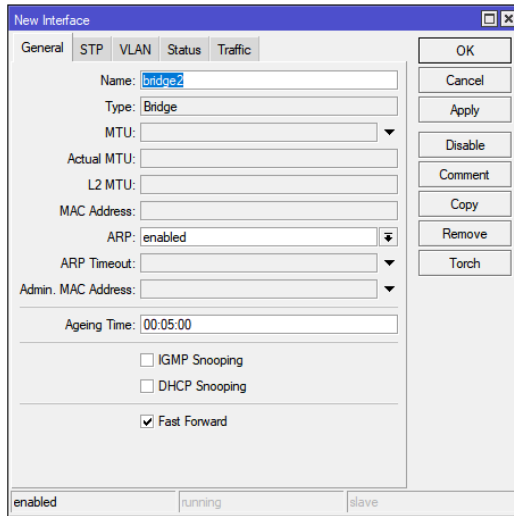
Gambar 3. 25 Tampilan DHCP Setup Bridge Next5



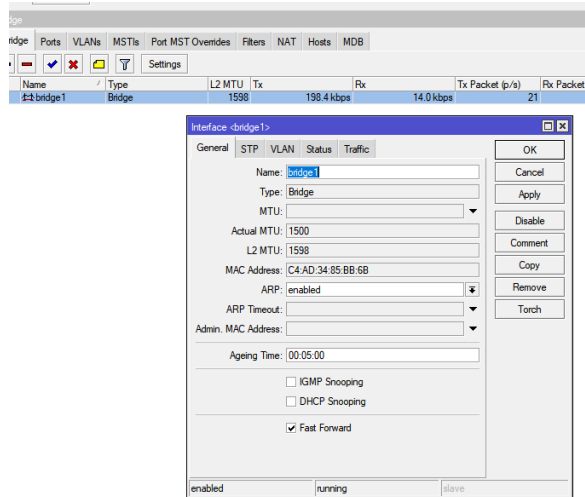
Gambar 3. 26 Tampilan DHCP Server



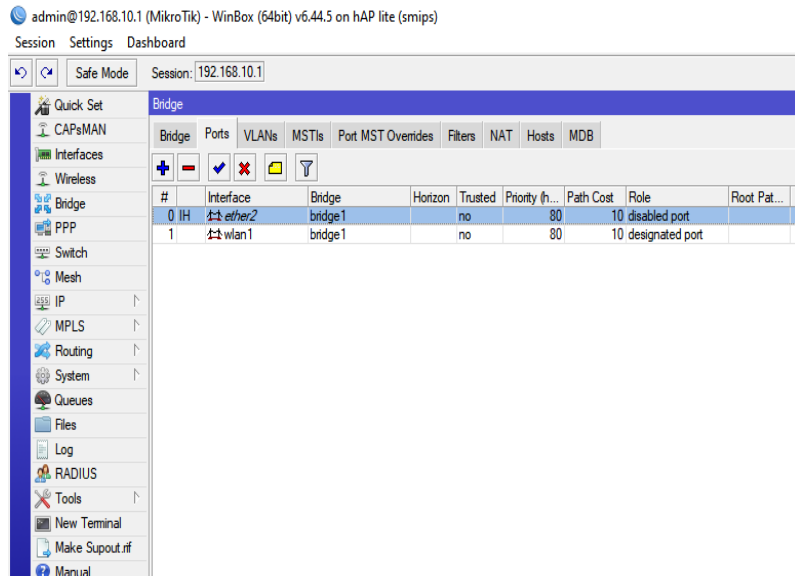
Gambar 3. 27 Tampilan Menu Bridge



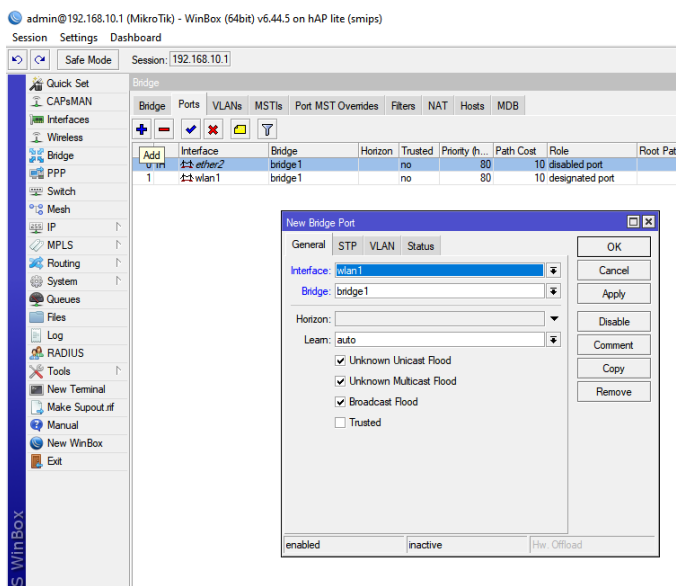
Gambar 3. 28 Tampilan Tambah Bridge



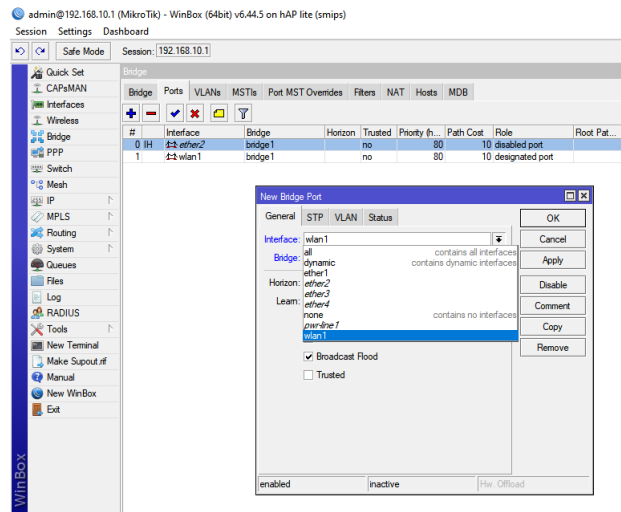
Gambar 3. 29 Tampilan Bridge1 Yang Sudah Ditambahkan Atau Dibuat



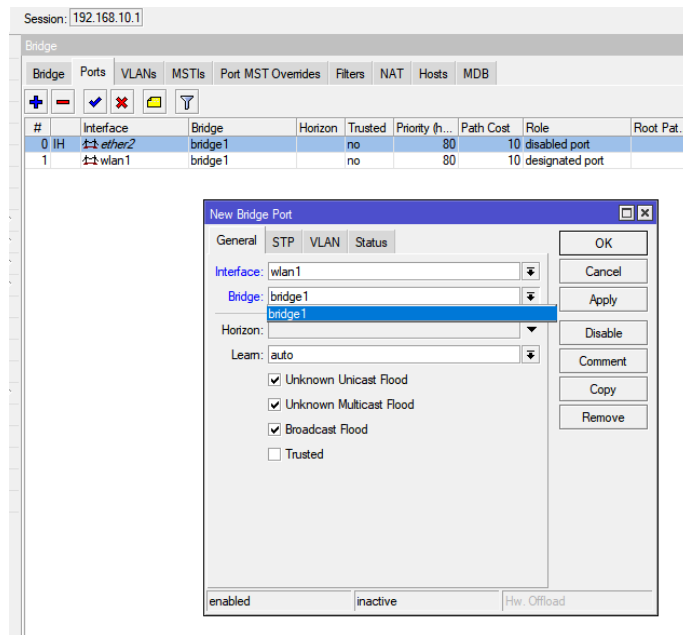
Gambar 3. 30 Tampilan Menu Bridge Pada Tab Ports



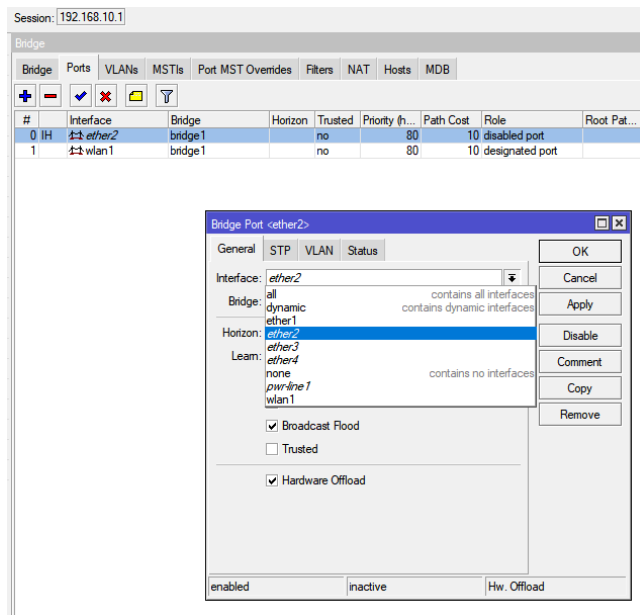
Gambar 3. 31 Tampilan Tambah Ports Pada Menu Bridge



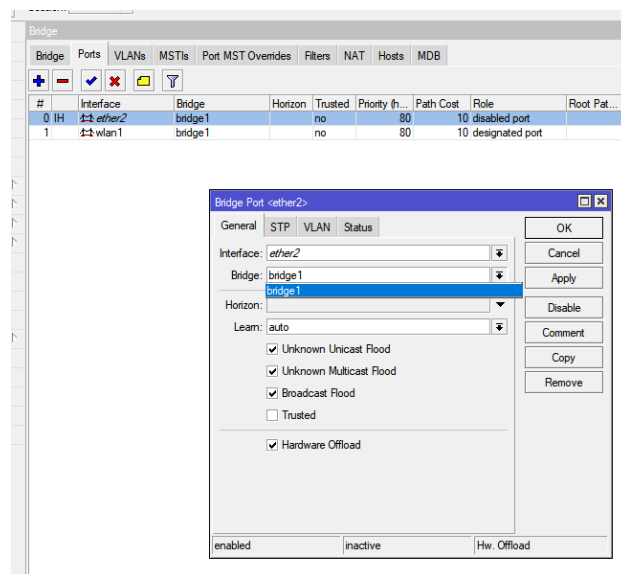
Gambar 3. 32 Tampilan Interfaces Pada Menu Port Pilih WLAN1 Untuk Membuat WIFI Lokal Menggunakan Bridge



Gambar 3. 33 Tampilan Bridge Yang Sudah Dibuat Sebelumnya Untuk Membuat Wifi Lokal



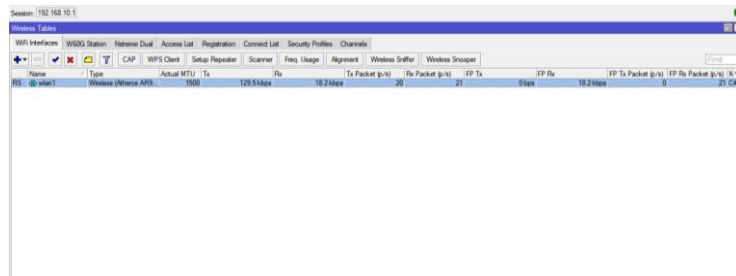
Gambar 3. 34 Tampilan Interfaces Pada Menu Port Pilih Ether2 Agar Client Terhubung Pada Jaringan WIFI Lokal Yang Dibuat Menggunakan Bridge



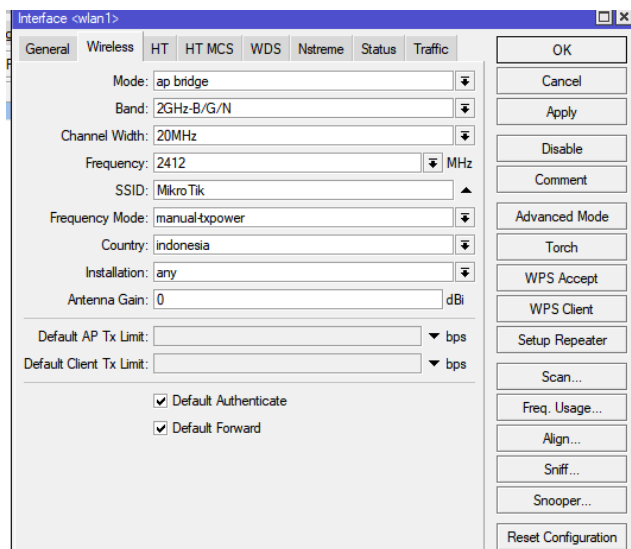
Gambar 3. 35 Tampilan Bridge Yang Sudah Dibuat Sebelumnya Untuk Membuat Wifi Lokal Yang Akan Terhubung Pada Client

2. Setting WIFI lokal

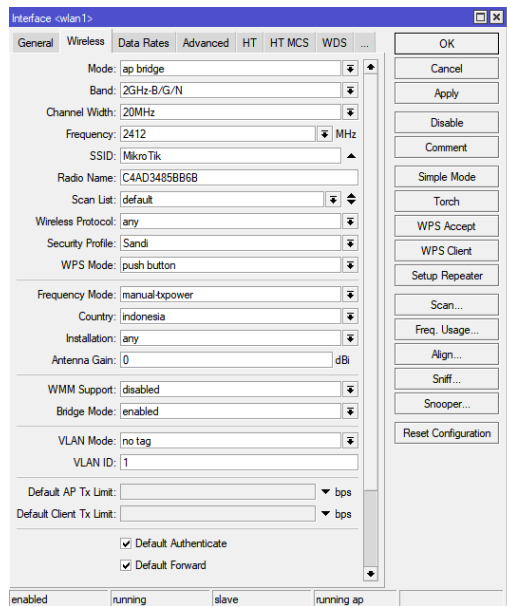
Lalu untuk membuat sebuah Wifi Local yang nantinya akan terhubung pada client Lokal dapat dilakukan dengan masuk pada menu Wireless dan pilih pada Tabnya Wifi Interfaces. Pilih Wlan1 klik lalu pada menu Wireless pilih Advanced Mode untuk mengatur wifi lokal yang dibuat secara lengkap. Pada mode pilih ap bridge, Pada Band Pilih 2Ghz-B/G/N, Channel Width pilih 20 MHz, Frequency pilih 2412 berikan Country indonesia serta buat nama wifi lokal pada SSID isi sesuai keinginan, bila sudah klik Ok. Maka wifi lokal disini sudah ada dan terbentuk tetapi masih belum memiliki keamanan katasandi ataupun password dan sudah mempunyai koneksi atau akses internet yang tadi diberikan oleh modem wifi atau isp (wlan1 masih belum berfungsi). Untuk membuat wifi lokal dapat terkoneksi internet maka nantinya pada ip Firewall nat dapat ditambahkan akses menuju ke wifi lokal dan untuk membuat kata sandi bisa dilakukan pada menu wirelles pilih pada tab yang ada di atas Security profile.



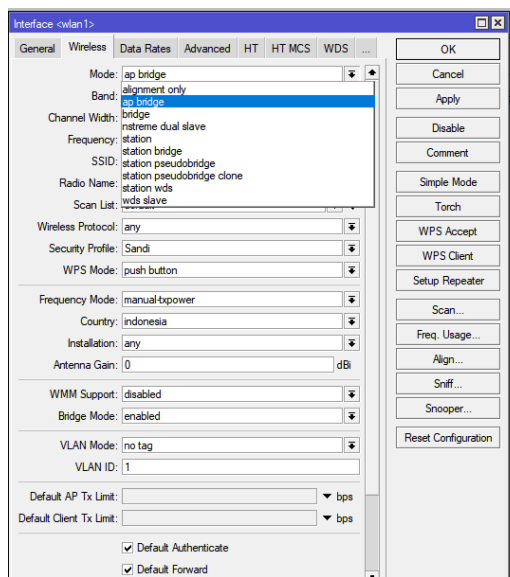
Gambar 3. 36 Tampilan Menu WLAN1 Atau WIFI Modem Yang Terhubung Ke Internet Yang Akan Digunakan Sebagai Bridge Ke Jaringan Wifi Lokal



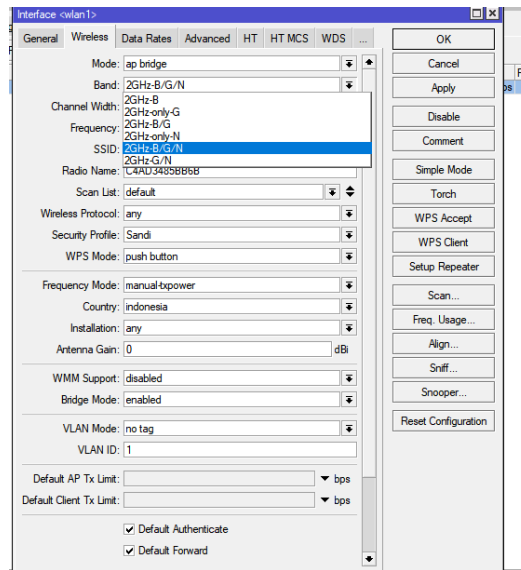
Gambar 3. 37 Tampilan Pengaturan Wlan1 Pada Mikrotik Simple Mode



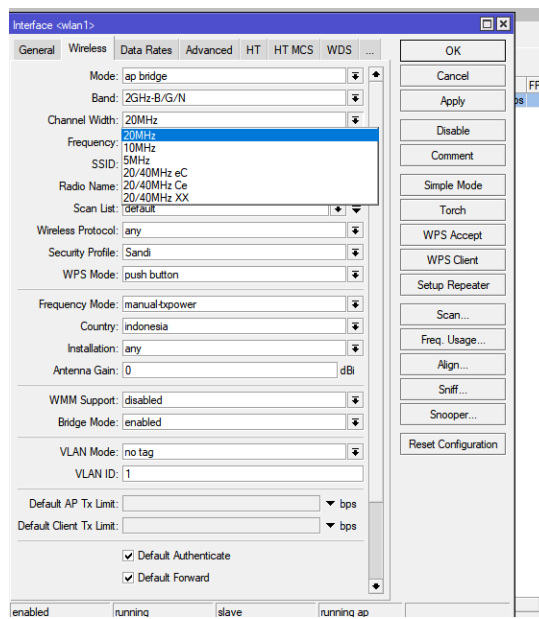
Gambar 3. 38 Tampilan Pengaturan Wlan1 Pada Mikrotik Advanced Mode



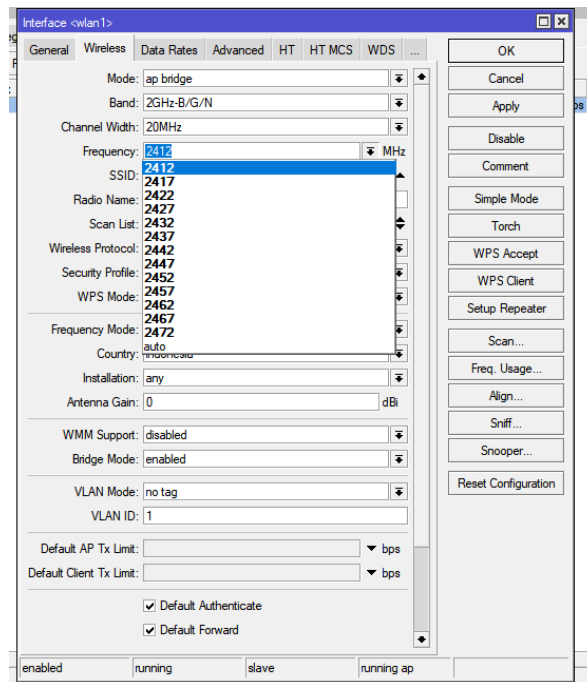
Gambar 3. 39 Tampilan Ubah Mode Wlan1 Menjadi Ap Bridge



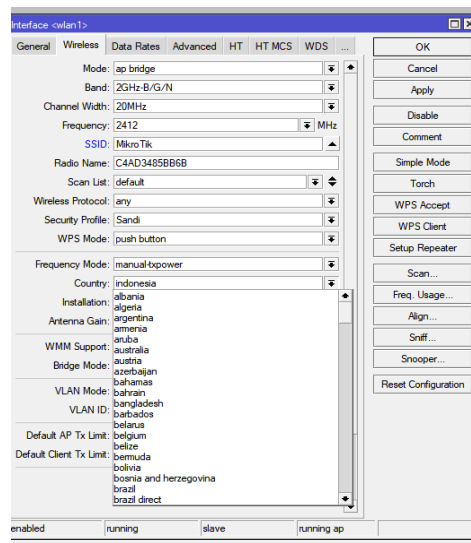
Gambar 3. 40 Tampilan Ubah Band Wlan1 Menjadi 2ghz-B/G/N



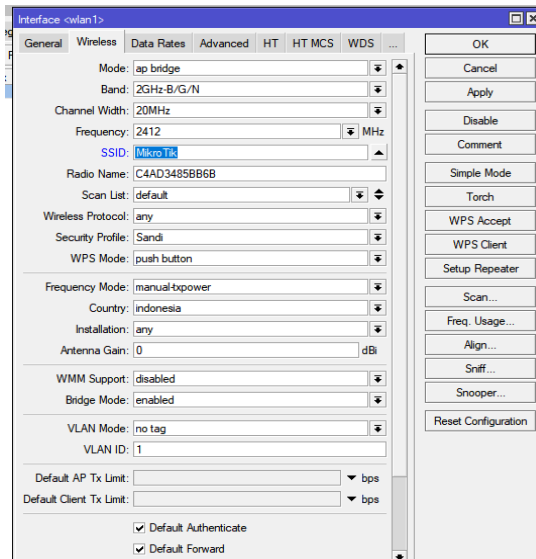
Gambar 3. 41 Tampilan Ubah Channel Width Menjadi 20 MH



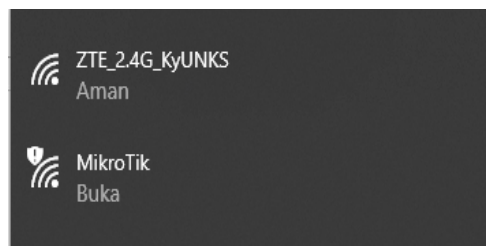
Gambar 3. 42 Tampilan Ubah Frequency Menjadi 2412



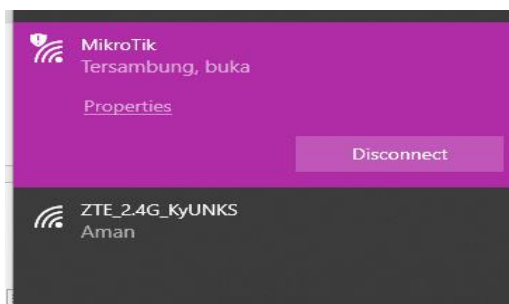
Gambar 3. 43 Tampilan Pilih Country Indonesia Pada Wlan1



Gambar 3. 44 Tampilan Buat SSID Untuk Nama Wifi Lokal



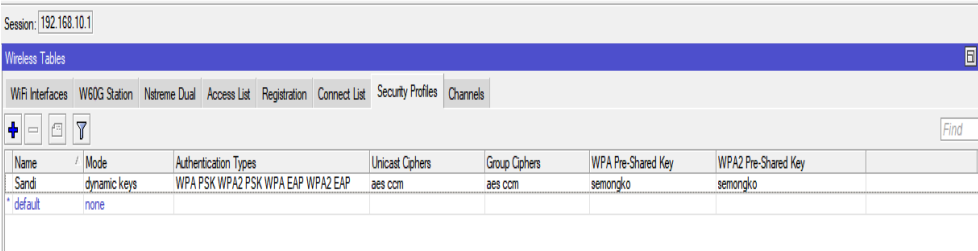
Gambar 3. 45 Tampilan Wifi Belum Memiliki Keamanan Kata Sandi Maupun Password



Gambar 3. 46 Tampilan Wifi Dapat Diakses Siapa Saja Dan Lemah Keamanan

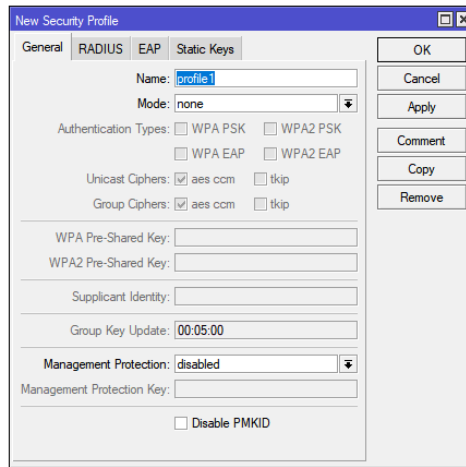
3. Setting password

Disini wifi lokal akan terlihat belum memiliki keamanan kata sandi atau Password, untuk memberikan Password pada Wifi Lokal yang dibuat pilih menu wireless maka Wireless Tables lalu pada tab tablenya klik Security Profiles maka bila belum menambahkan katasandi pada Wrelles Tables hanya akan terlihat default. Untuk menambahkan klik tanda + pada general name berikan nama terserah yang akan diinginkan, pada Mode pilih Dynamic Keys dan Centang semua Authentication Types yang ada. Lalu berikan katasandi atau buat katasandi atau password untuk keamanan Wifi lokal yang dibuat pada WPA Pre-shared key dan ulangi sandi pada WPA2 Pre-shared key lalu klik OK. Pada Wireless Tables pilih Wifi Interface untuk memasukkan katasandi yang sudah dibuat sebelumnya. Klik Wlan1 pada Security Profile pilih nama yang tadi dibuat pada security profile disini penulis membuat dan memberikan nama sandi, bila sudah klik OK. Bila sebelumnya Pada DHCP Server memilih Ether2 maka sekarang ubah menjadi Brigde1. Lalu next next sampai selesai

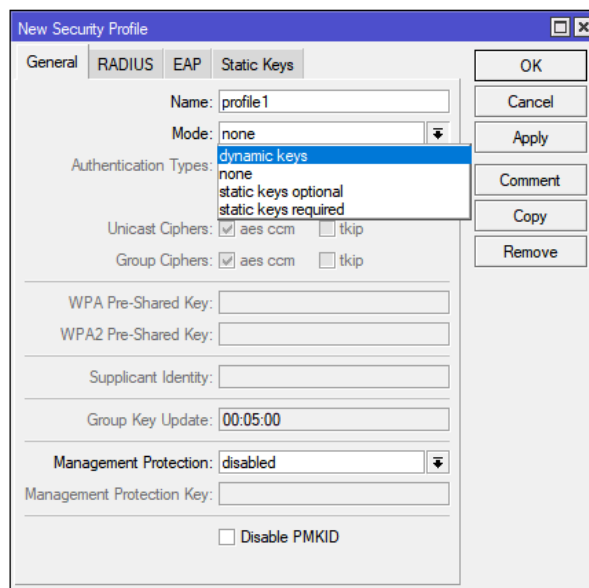


Name	Mode	Authentication Types	Unicast Ciphers	Group Ciphers	WPA Pre-Shared Key	WPA2 Pre-Shared Key
Sandi	dynamic keys	<input checked="" type="checkbox"/> WPA PSK <input checked="" type="checkbox"/> WPA2 PSK <input checked="" type="checkbox"/> WPA EAP <input checked="" type="checkbox"/> WPA2 EAP	aes ccm	aes ccm	semongko	semongko
* default	none					

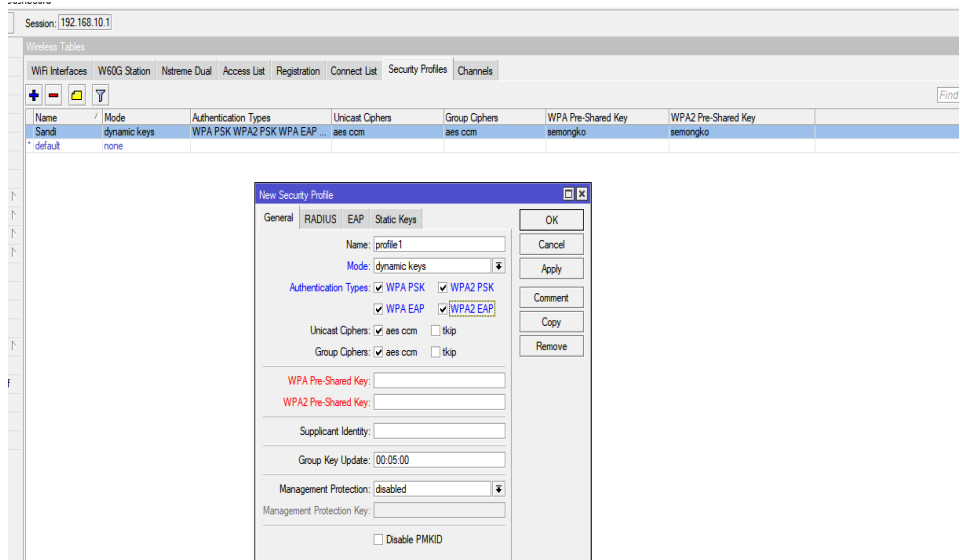
Gambar 3. 47 Buat Sandi Wifi Lokal Pada Tab Security Profile



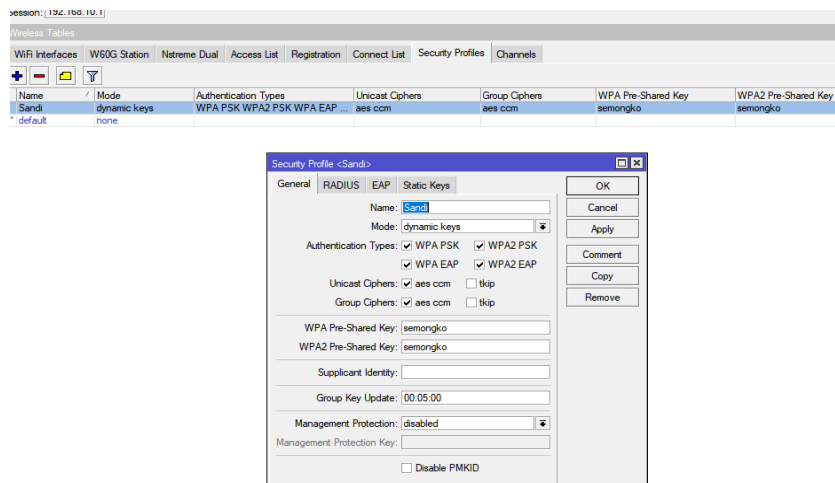
Gambar 3. 48 Tampilan Tambah Kata Sandi Berikan Nama Pada Name



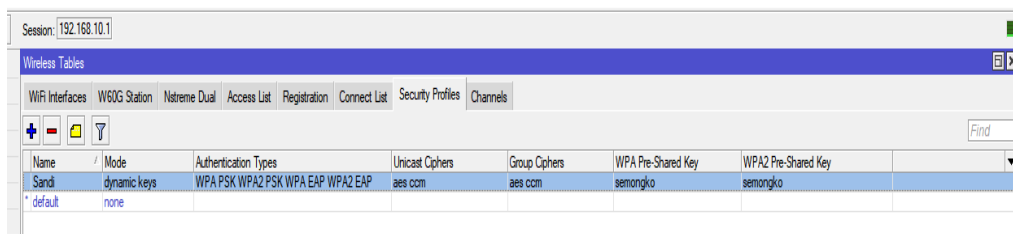
Gambar 3. 49 Tampilan Tambah Kata Sandi Pilih Dynamic Keys



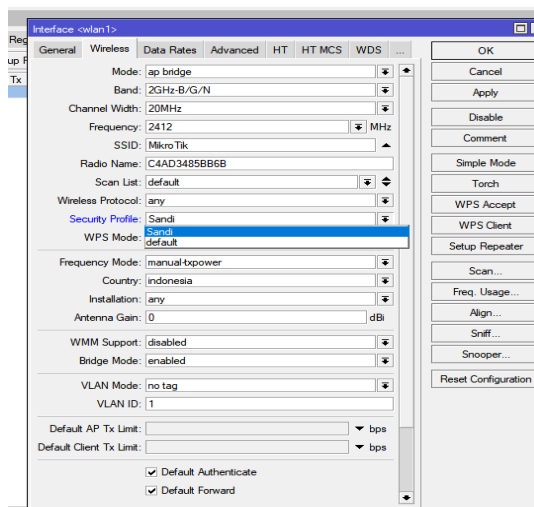
Gambar 3. 50 Tampilan Tambah Kata Sandi Ceklis Semua Authentication



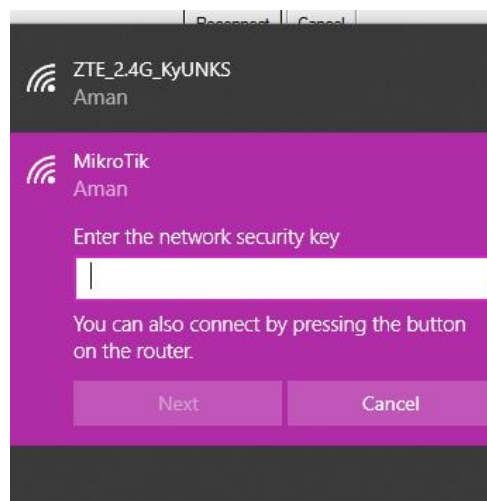
Gambar 3. 51 Tampilan Buat Sandi Pada Wifi Lokal



Gambar 3. 52 Tampilan Security Profile Yang Sudah Dibuat



Gambar 3. 53 Tampilan Wlan1 Pada Wireless Ubah Security Profile Dengan Yang Tadi Sudah Dibuat (Name= Sandi)



Gambar 3. 54 Tampilan Wifi Lokal Mikrotik Dengan Memiliki Sandi Yang Sudah Dibuat Dan Dimasukkan Dalam Pengaturan Winbox Di Mikrotik

g. Setting Mangle dan Queue

Pengaturan mangle dan queue digunakan untuk mengatur atau memajemen bandwidth yang digunakan untuk menandai, membatasi dan menentukan jenis paket yang akan diakses oleh client atau user.

bandwidth total yang tersedia sebesar 400 kbps untuk downlink maupun uplink. Karena terdapat 3 client maka masing-masing client akan mendapatkan bandwidth sebesar 133,3 kbps. Jika hanya dua client yang aktif maka akan mendapatkan bandwidth masing-masing 200 kbps. Bandwidth ini berlaku untuk semua jenis paket data. Oleh karena itu perlu diatur manajemen bandwidth berdasarkan tipe datanya. Dengan bandwidth total 400 kbps berikut rincian masing-masing bandwidth berdasarkan tipe data.

- a) TCP : 150 kbps (up/down)
- b) UDP : 100 kbps (up/down)
- c) ICMP : 50 kbps (up/down)
- d) Sisa : 100 kbps (up/down)

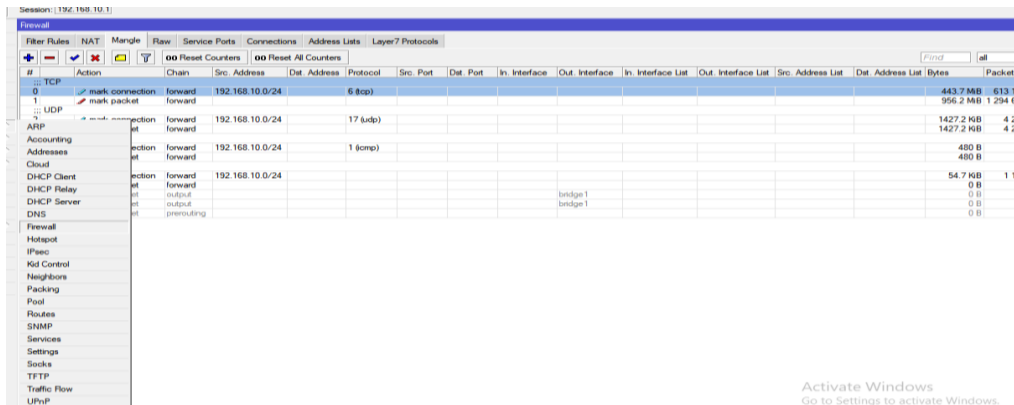
Bandwidth sisa digunakan untuk jenis paket yang lain.

1. Mangle

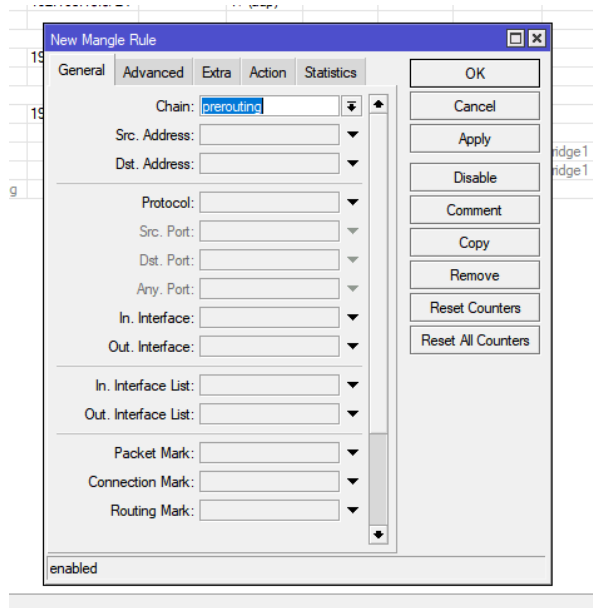
Cara melakukan pengaturan pada mangle dapat dilakukan pada menu ip pilih firewall dan pada tab firewall pilih mangle, bila sudah buat aturan mangle sesuai dengan aturan diatas atau kalau mau mengatur sendiri sesuai keinginan juga bisa, tetapi penulis disini menggunakan aturan yang diatas. Bila sudah terbuka jendela mangle pilih general lalu masukkan pada form chain = forward src. Address = sesuai dengan ip client yang sudah dibuat sebelumnya (192.168.10.0/24) protocol = tcp

lalu pindah ke menu Action isi chain = mark connection new connection mark= conn-tcp (tulis), lalu centang pada passthrough atau connection passthrough yes kemudian OK. Jangan lupa untuk membuat comment agar tidak kebingungan dengan banyak setingan dengan cara pilih comment pada tab yang sejajar dengan menu ok lalu berikan nama.

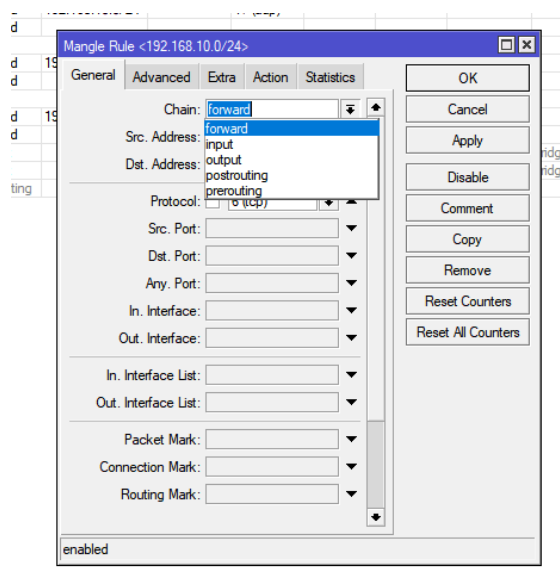
Dengan langkah yang sama buat packet data pada ip firewall mangle pilih general dan masukan chain = forward connection mark = conn tcp kemudian pindah pada menu action = mark packet new packet mark = packet-tcp (tulis), lalu pada passthrough atau connection passthrough no atau biarkan kosong kemudian OK. Lakukan hal yang sama pada mangle packet UDP, ICMP dan sisa dengan mark connection 17 untuk UDP, 1 untuk ICMP dan kosongkan untuk sisa.



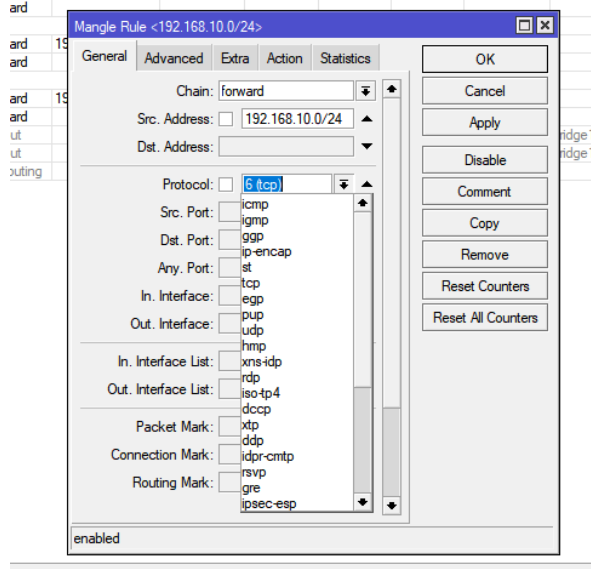
Gambar 3. 55 Tampilan Pengaturan Ip Firewall Mangle



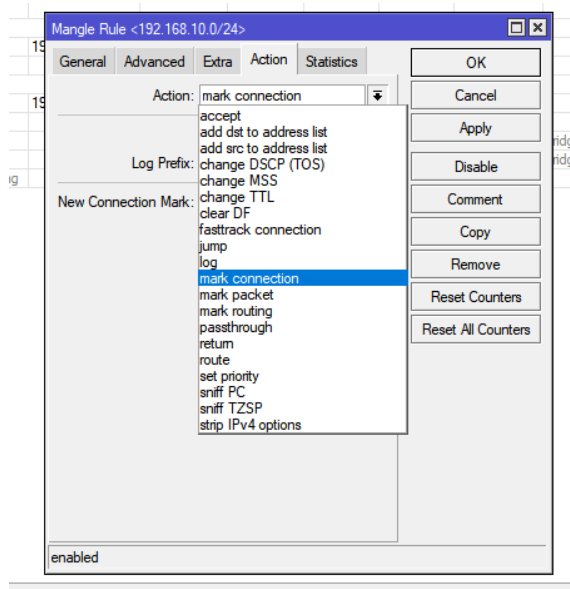
Gambar 3. 56 Tampilan Untuk Menambahkan Mangle Sesuai Aturan Sendiri



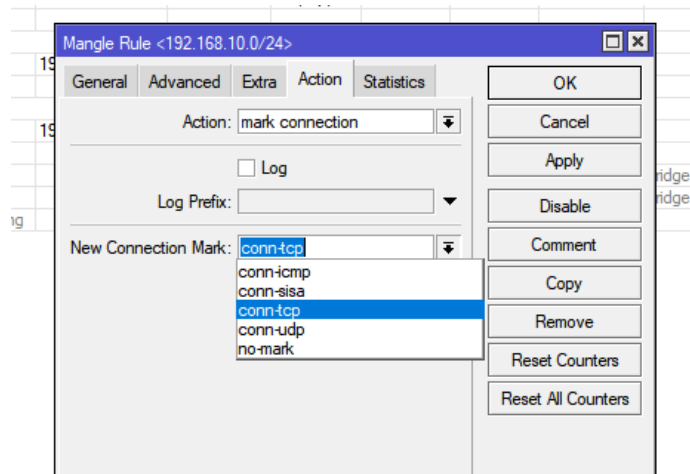
Gambar 3. 57 Tampilan Mangle Packet Tcp Mark Connection General Chain Pilih Forward



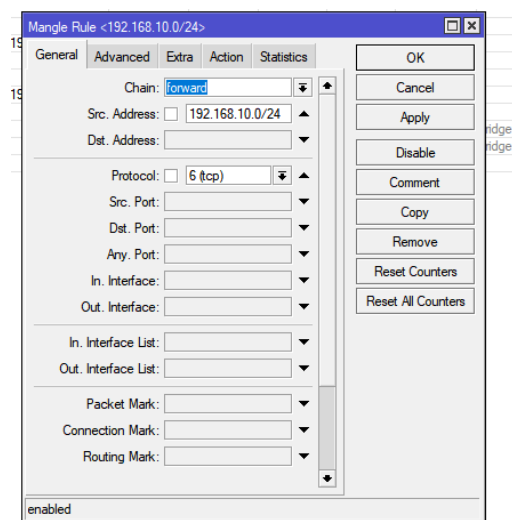
Gambar 3. 58 Tampilan Mangle Packet Tcp Mark Connection General Masukkan Protocol Sesuai Yang Diterapkan Dan Masukkan Ip Yang Digunakan Untuk Mengatur Client Pada Jaringan



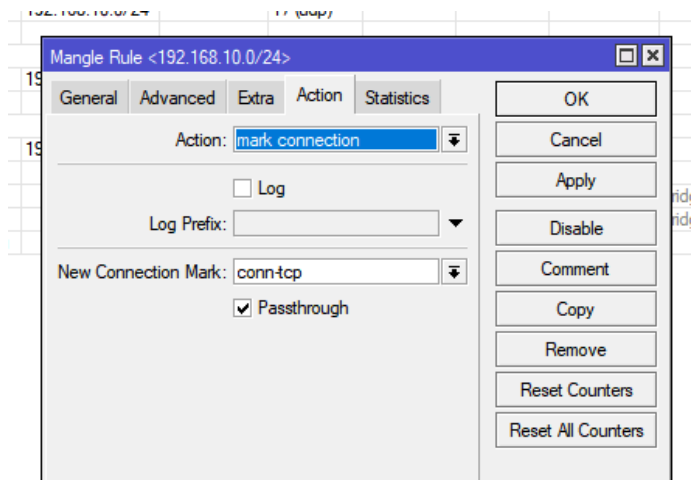
Gambar 3. 59 Tampilan Mangle Packet Tcp Action Mark Connection



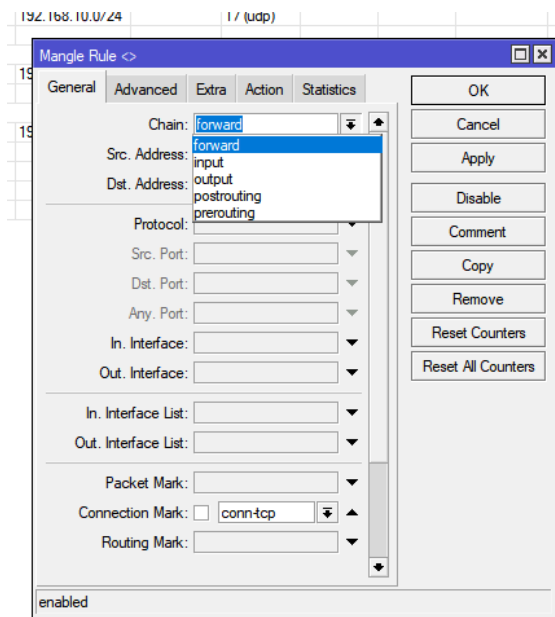
Gambar 3. 60 Tampilan Mangle Packet Tcp Action Conn-Tcp



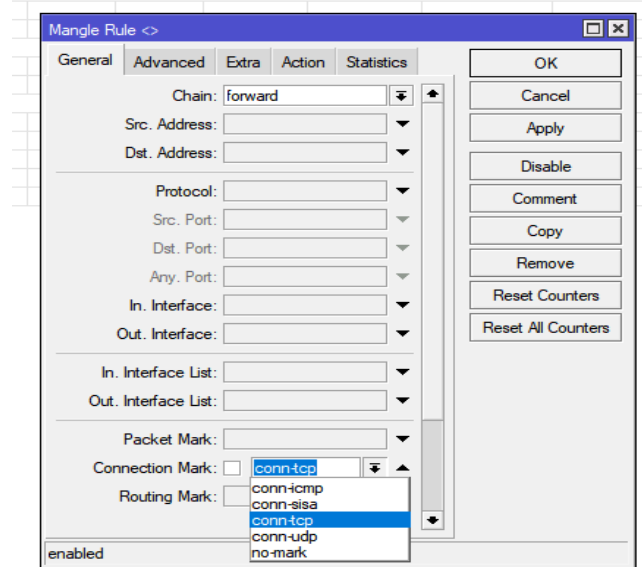
Gambar 3. 61 Tampilan Setting Packet Tcp Mangle Pada Tab General Mark Connection



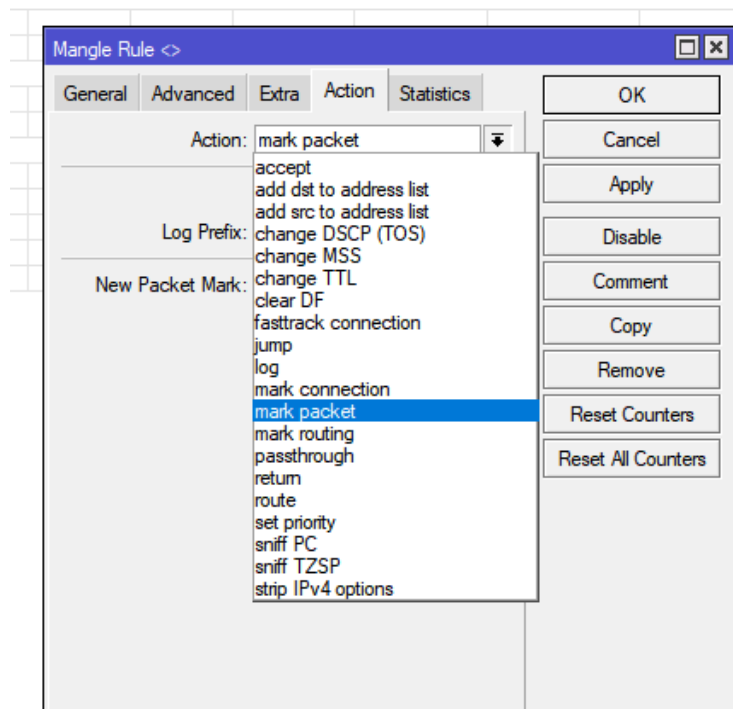
Gambar 3. 62 Tampilan Setting Packet Tcp Magle Pada Tab Action Mark Connection



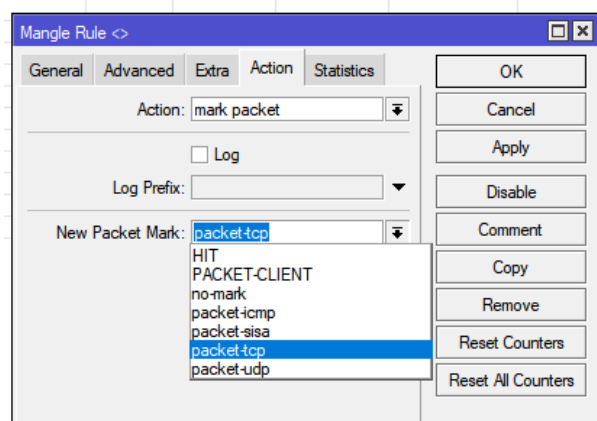
Gambar 3. 63 Tampilan Mangle Packet Tcp Mark Packet General Chain Pilih Forward



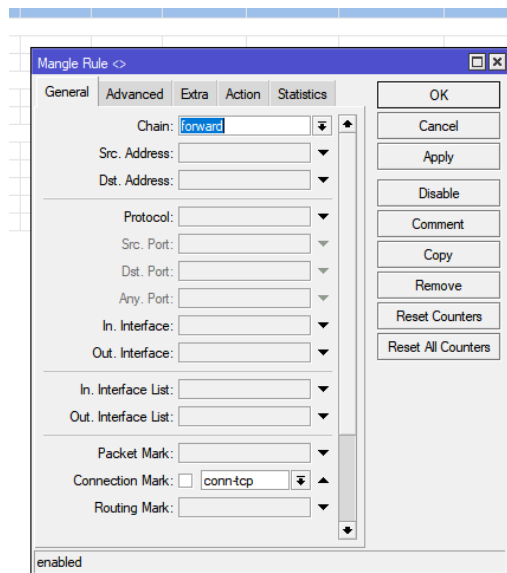
Gambar 3. 64 Tampilan Mangle Packet Tcp Mark Packet General Connection
Pilih Conn-Tcp



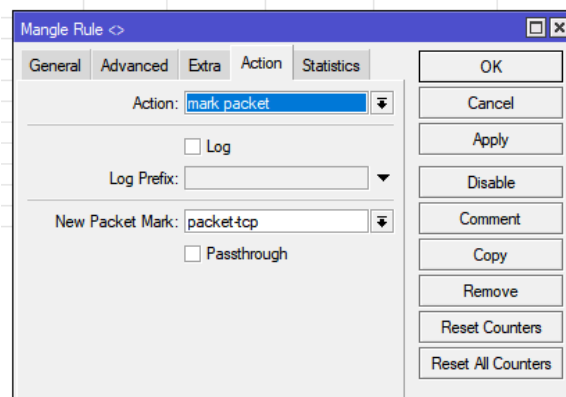
Gambar 3. 65 Tampilan Mangle Packet Tcp Action Mark Packet



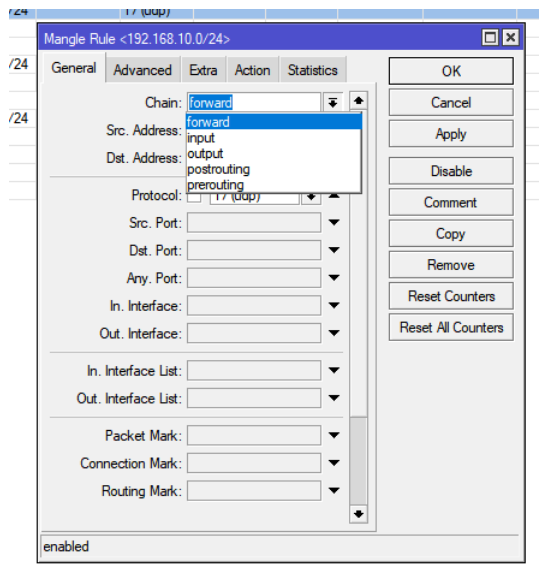
Gambar 3. 66 Tampilan Mangle Packet Tcp Action Packet-Tcp



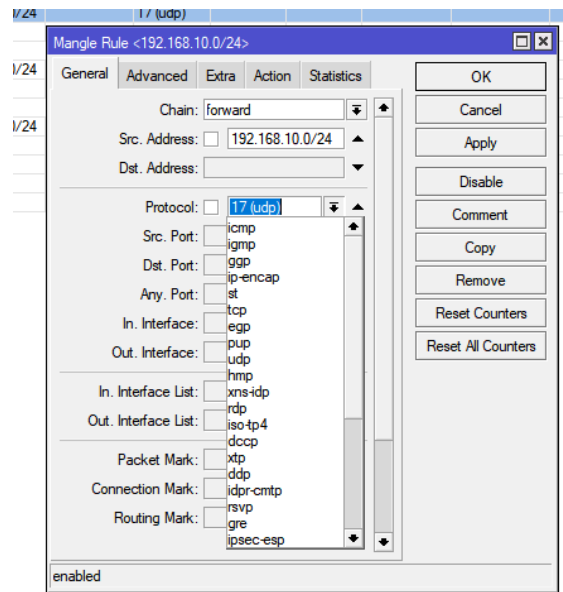
Gambar 3. 67 Tampilan Setting Packet Tcp Mangle Pada Tab General Mark Packet



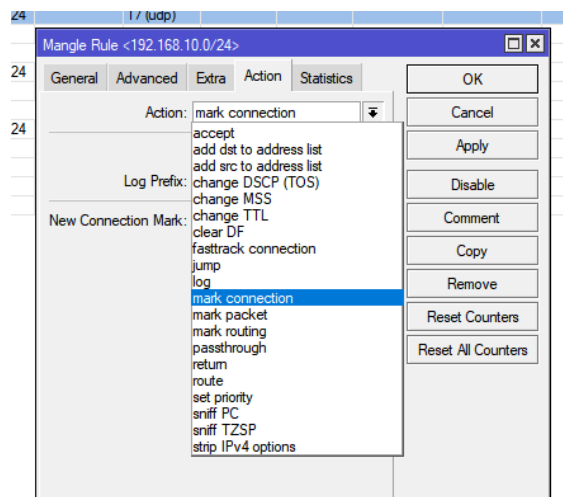
Gambar 3. 68 Tampilan Setting Packet Tcp Mangle Pada Tab Action Mark Packet



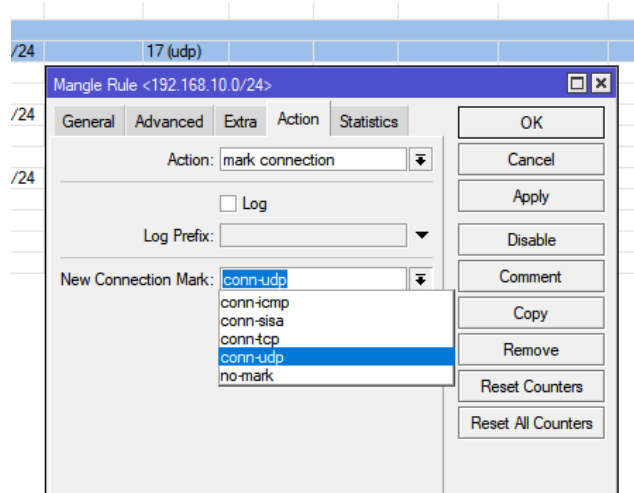
Gambar 3. 69 Tampilan Mangle Packet Udp Mark Connection General Chain
Pilih Forward



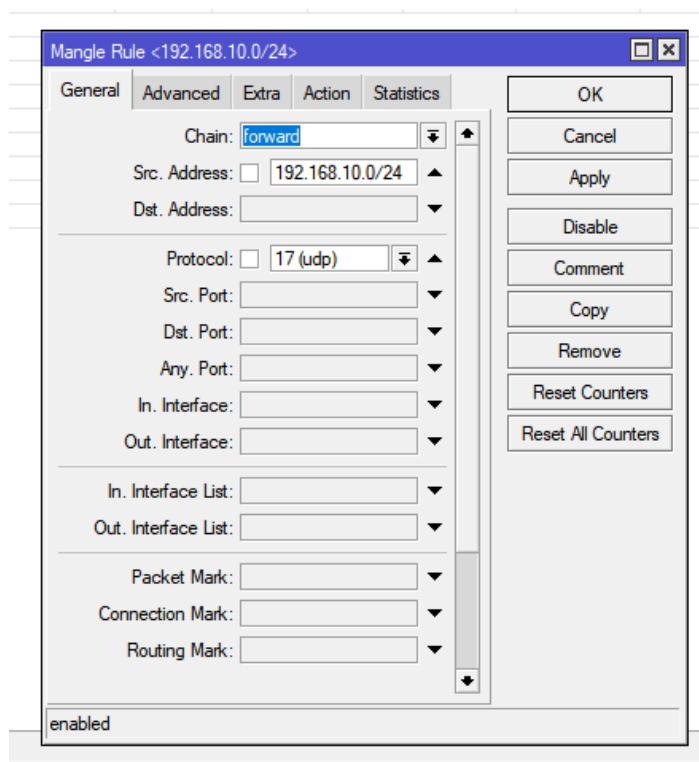
Gambar 3. 70 Tampilan Mangle Packet Udp Mark Connection General Masukkan Protocol Sesuai Yang Diterapkan Dan Masukkan Ip Yang Digunakan Untuk Mengatur Client Pada Jaringan



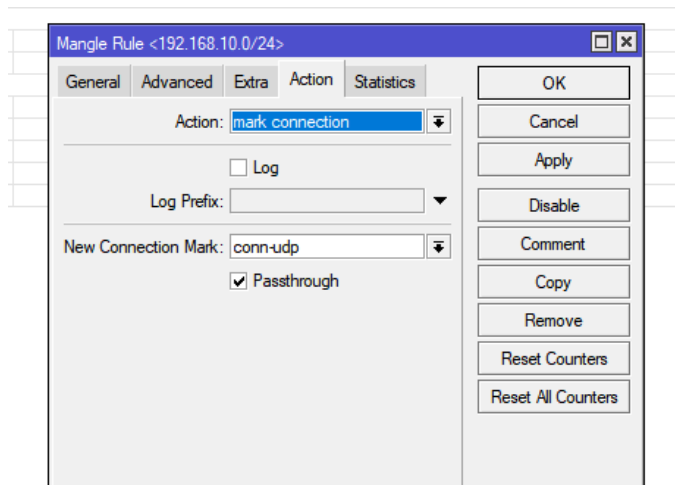
Gambar 3. 71 Tampilan Mangle Packet Udp Action Mark Connection



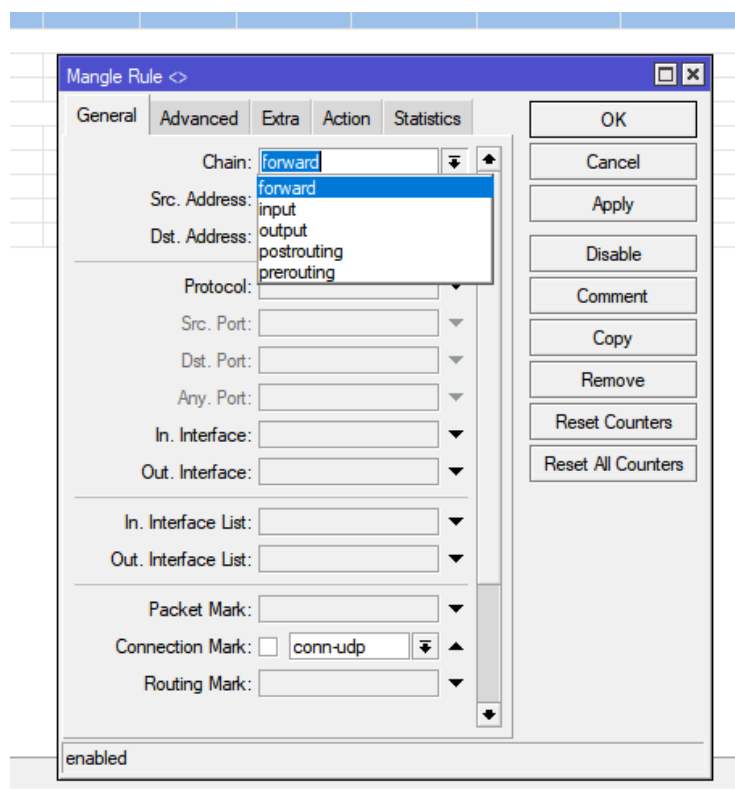
Gambar 3. 72 Tampilan Mangle Packet Udp Action Conn-Udp



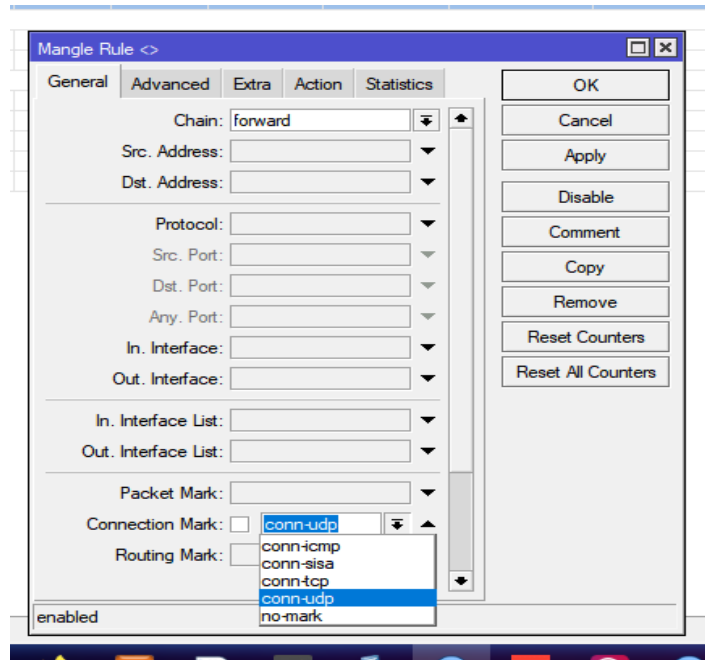
Gambar 3. 73 Tampilan Setting Packet Udp Mangle Pada Tab General Mark Connection



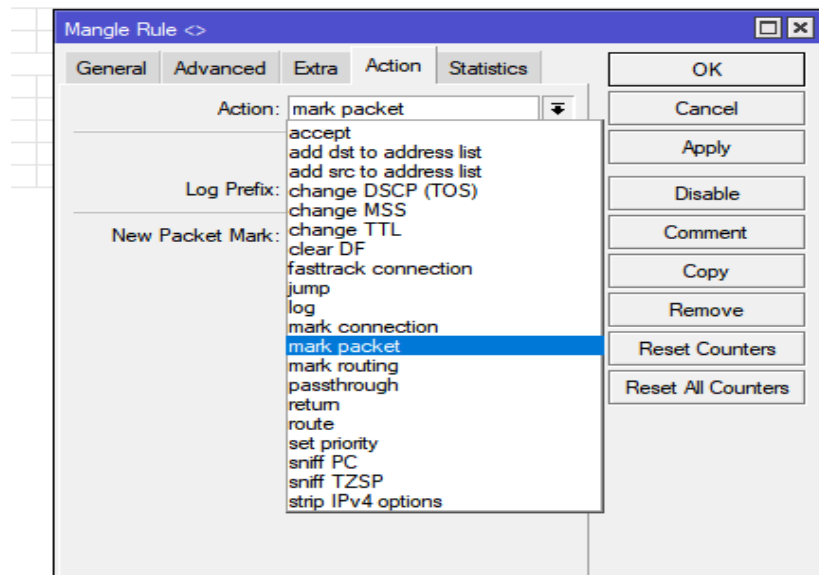
Gambar 3. 74 Tampilan Setting Packet Udp Mangle Pada Tab Action Mark Connection



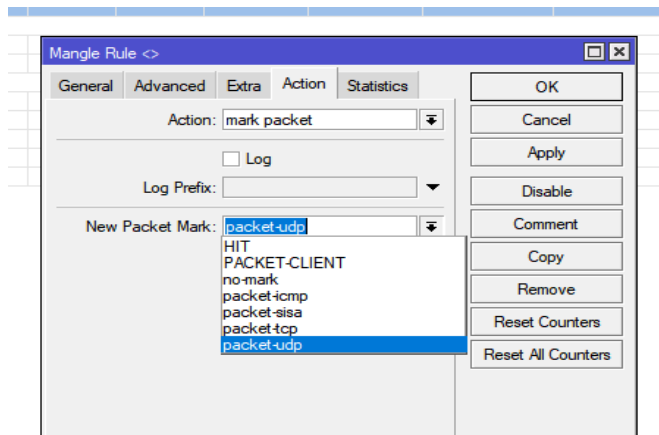
Gambar 3. 75 Tampilan Mangle Packet Udp Mark Packet General Chain Pilih Forward



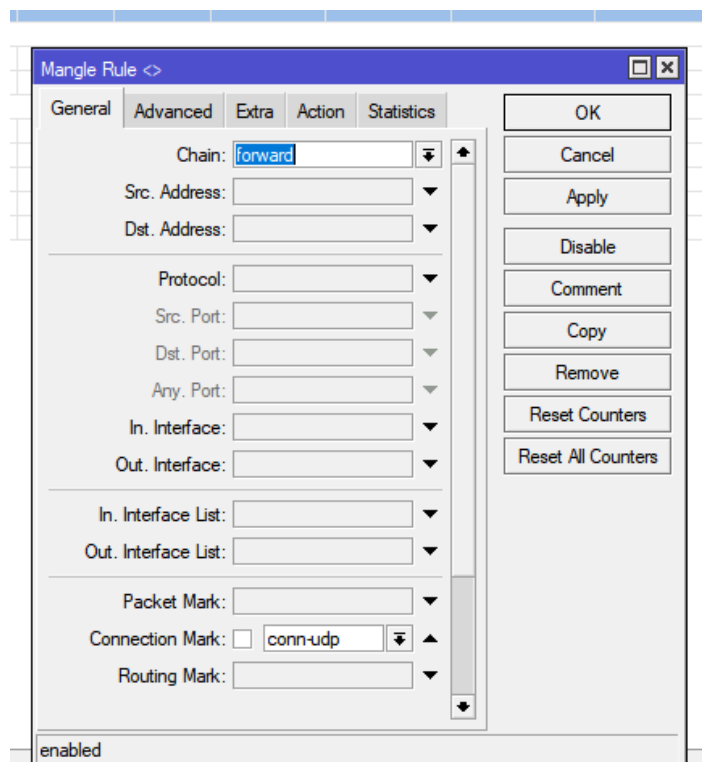
Gambar 3. 76 Tampilan Mangle Packet Udp Mark Packet General Connection
Pilih Conn-Udp



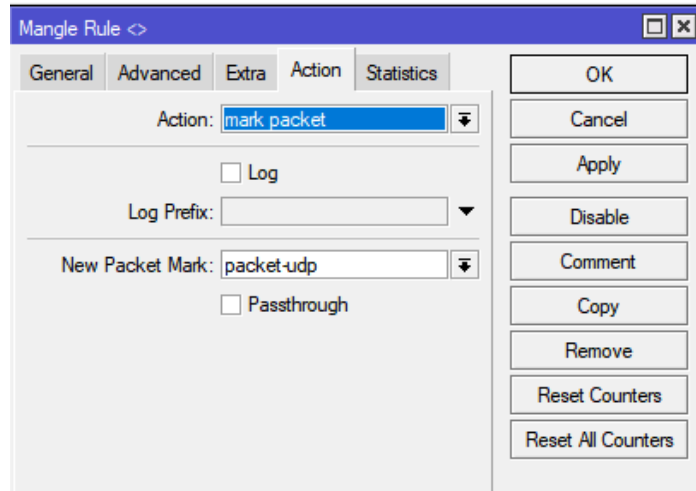
Gambar 3. 77 Tampilan Mangle Packet Udp Action Mark Packet



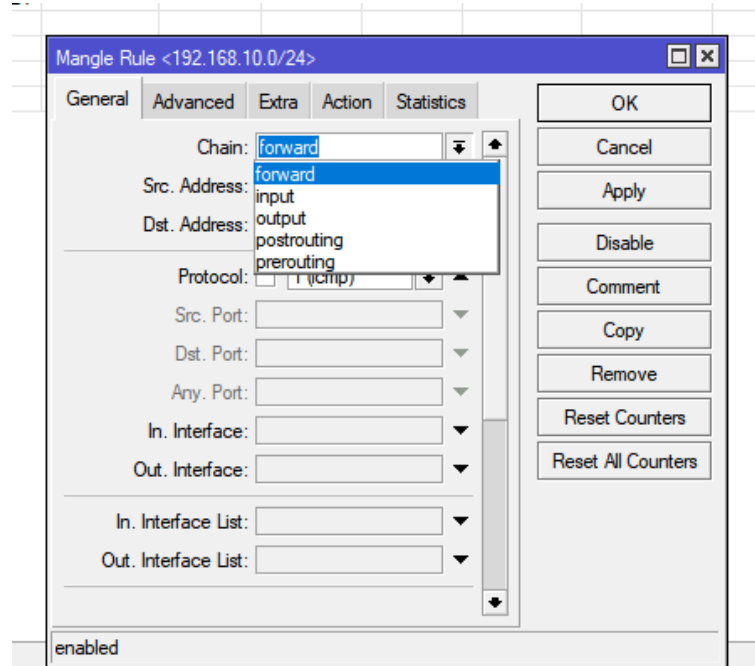
Gambar 3. 78 Tampilan Mangle Packet Udp Action Packet-Udp



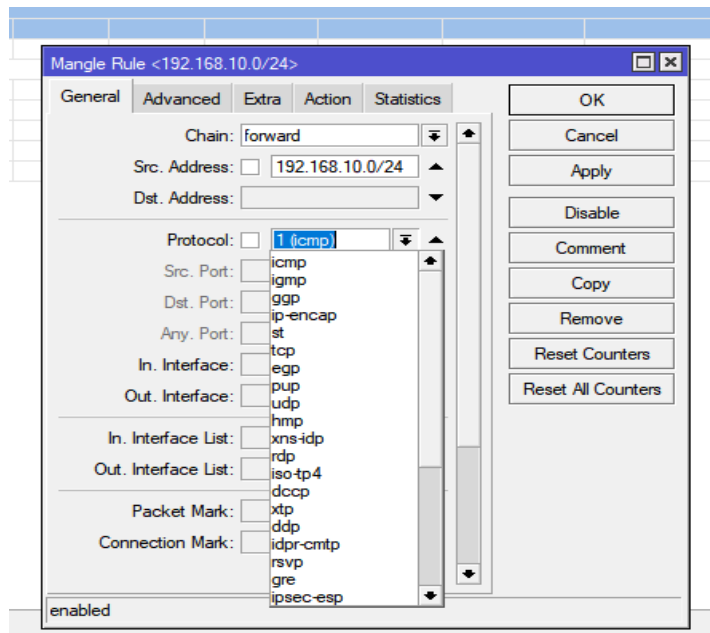
Gambar 3. 79 Tampilan Setting Packet Udp Mangle Pada Tab General Mark Packet



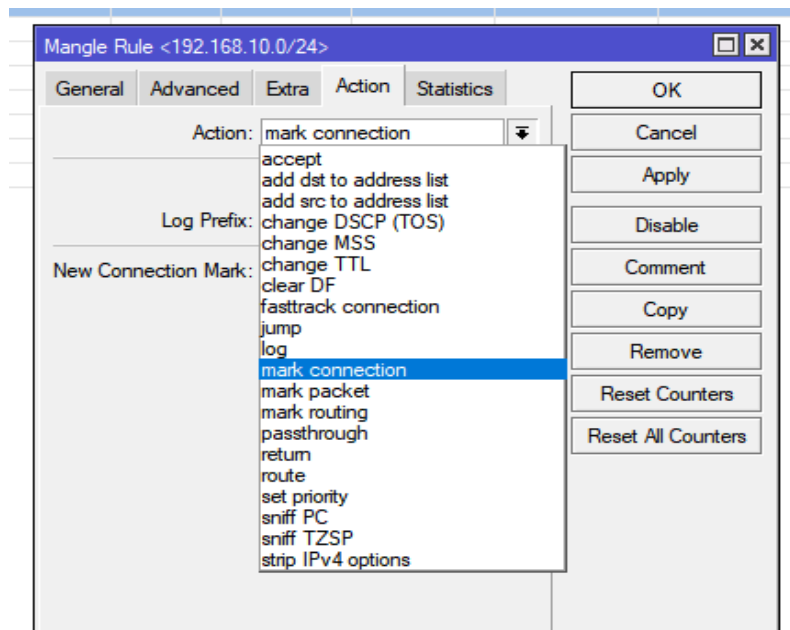
Gambar 3. 80 Tampilan Setting Packet Udp Mangle Pada Tab Action Mark Packet



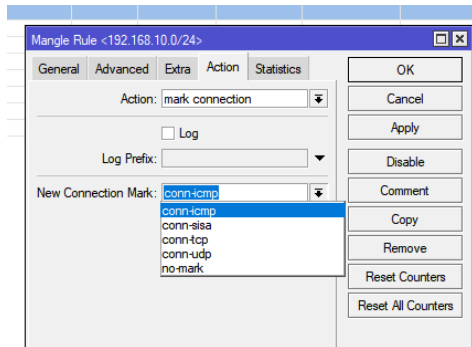
Gambar 3. 81 Tampilan Mangle Packet Icmp Mark Connection General Chain Pilih Forward



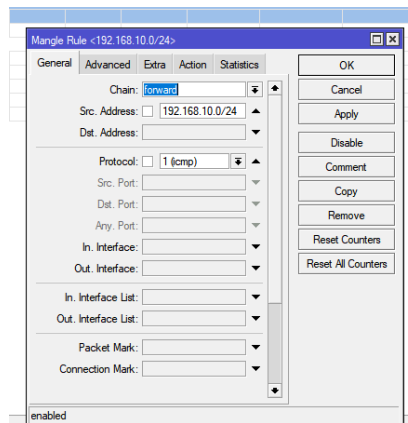
Gambar 3. 82 Tampilan Mangle Packet Icmp Mark Connection General
Masukkan Protocol Sesuai Yang Diterapkan Dan Masukkan Ip Yang Digunakan
Untuk Mengatur Client Pada Jaringan



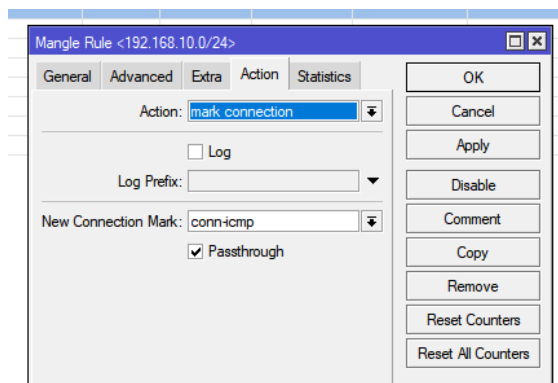
Gambar 3. 83 Tampilan Mangle Packet Icmp Action Mark Connection



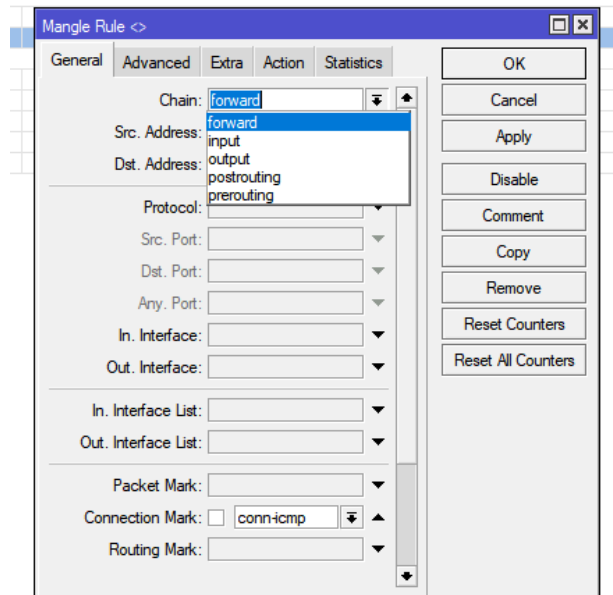
Gambar 3. 84 Tampilan Mangle Packet Icmp Action Conn-Icmp



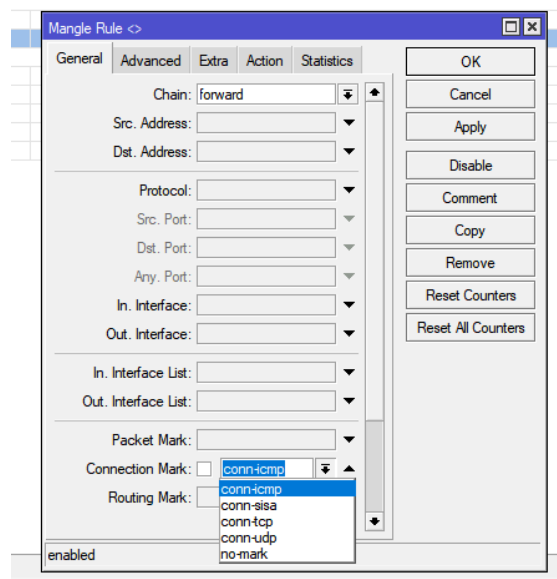
Gambar 3. 85 Tampilan Setting Packet Icmp Mangle Pada Tab General Mark Connection



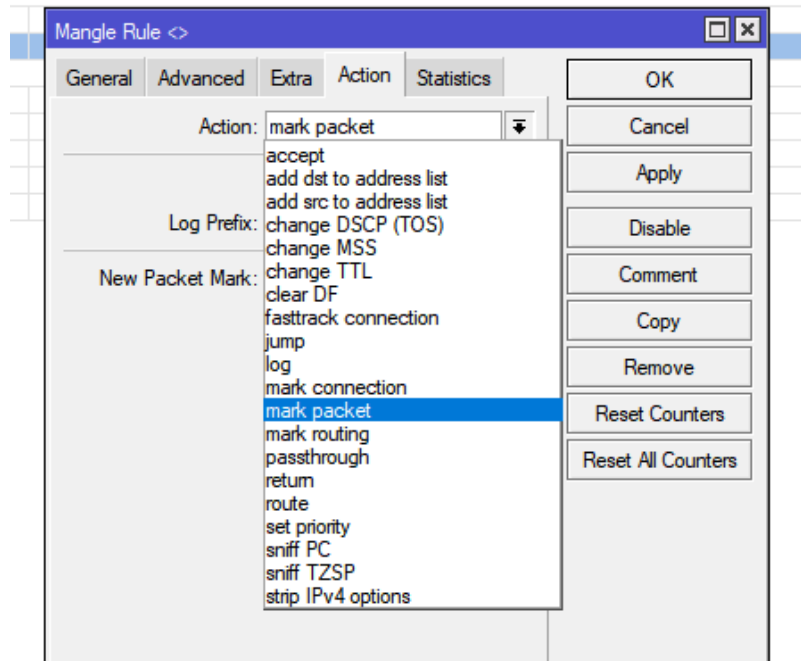
Gambar 3. 86 Tampilan Setting Packet Icmp Mangle Pada Tab Action Mark Connection



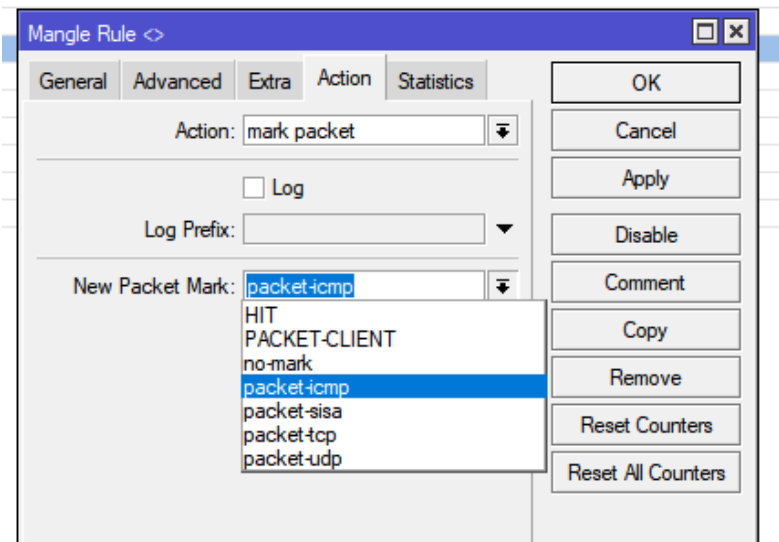
Gambar 3. 87 Tampilan Mangle Packet Icmp Mark Packet General Chain Pilih Forward



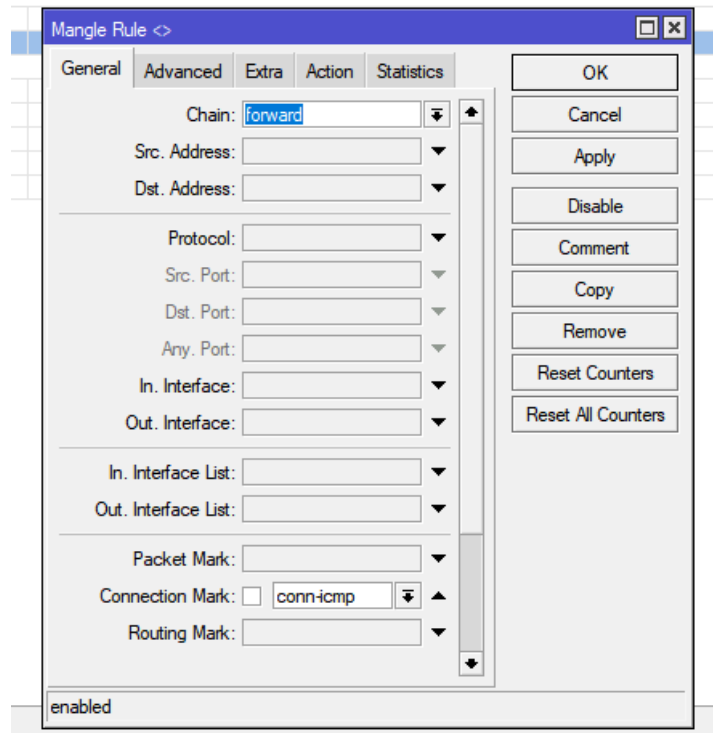
Gambar 3. 88 Tampilan Mangle Packet Icmp Mark Packet General Connection Pilih Conn-Icmp



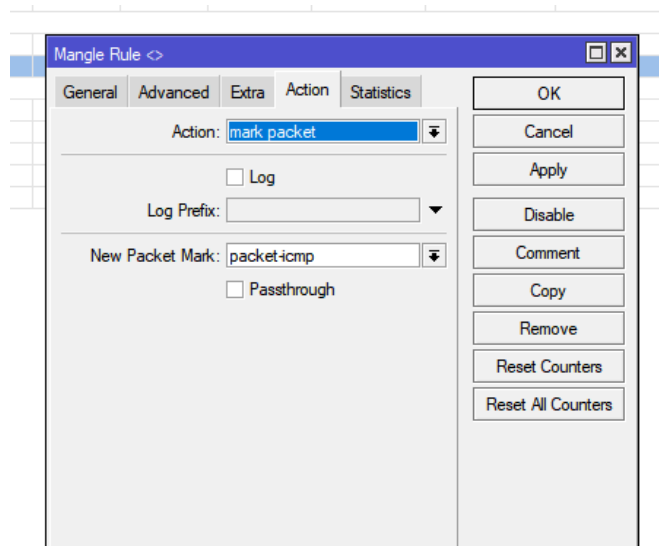
Gambar 3. 89 Tampilan Mangle Packet Icmp Action Mark Packet



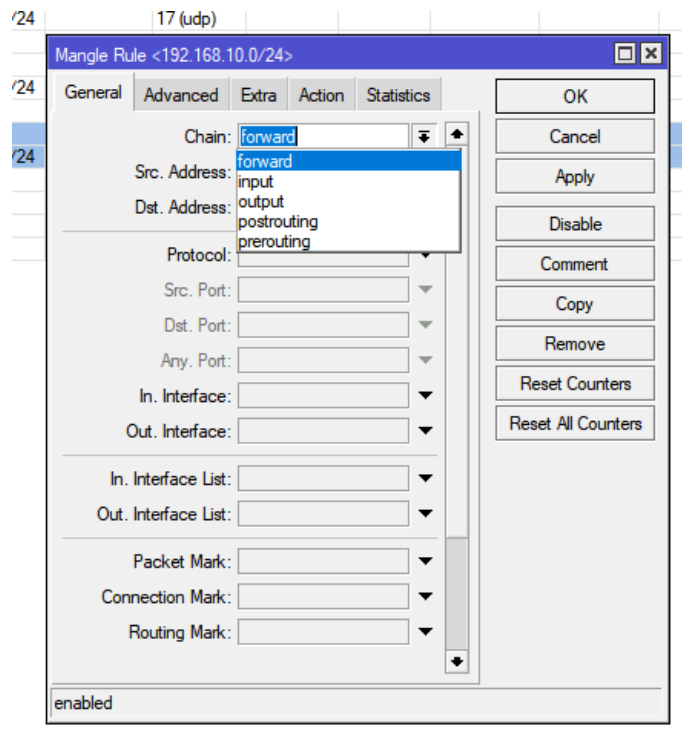
Gambar 3. 90 Tampilan Mangle Packet Icmp Action Packet-Icmp



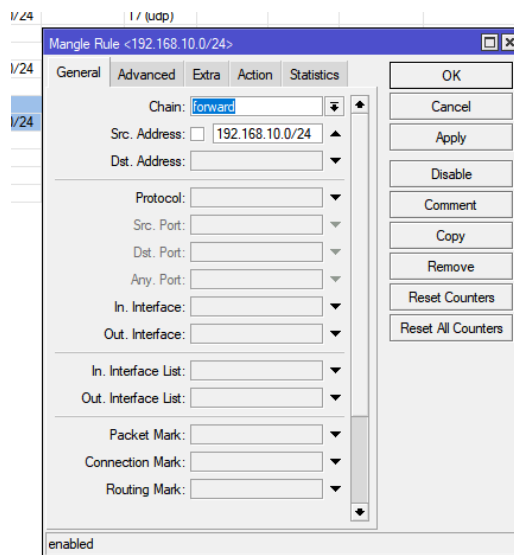
Gambar 3. 91 Tampilan Setting Packet Icmp Mangle Pada Tab General Mark Packet



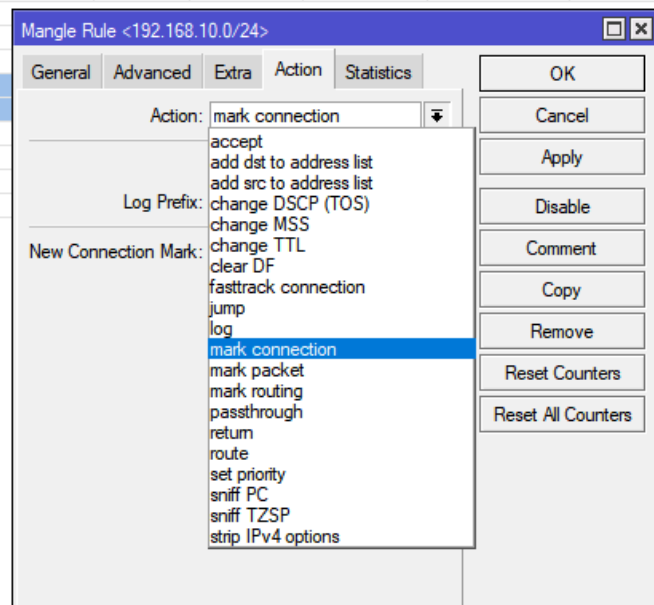
Gambar 3. 92 Tampilan Setting Packet Icmp Magle Pada Tab Action Mark Packet



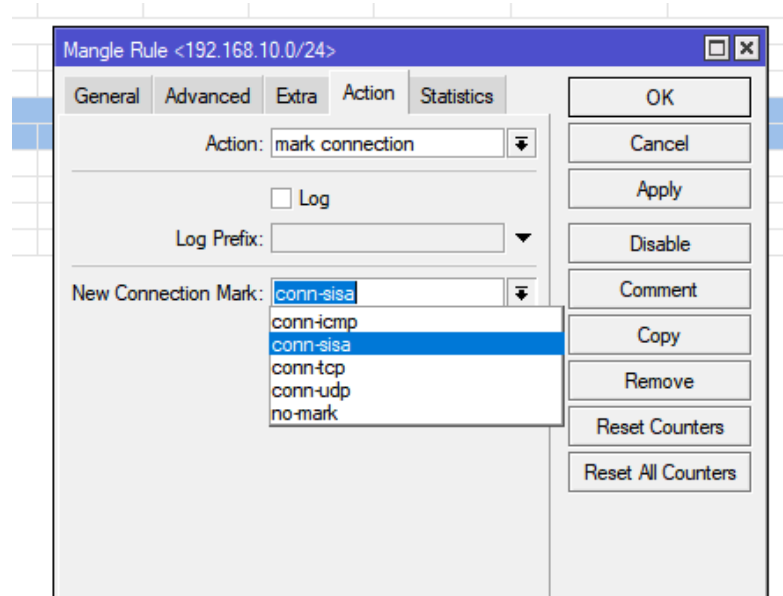
Gambar 3. 93 Tampilan Mangle Packet Sisa Mark Connection General Chain
Pilih Forward



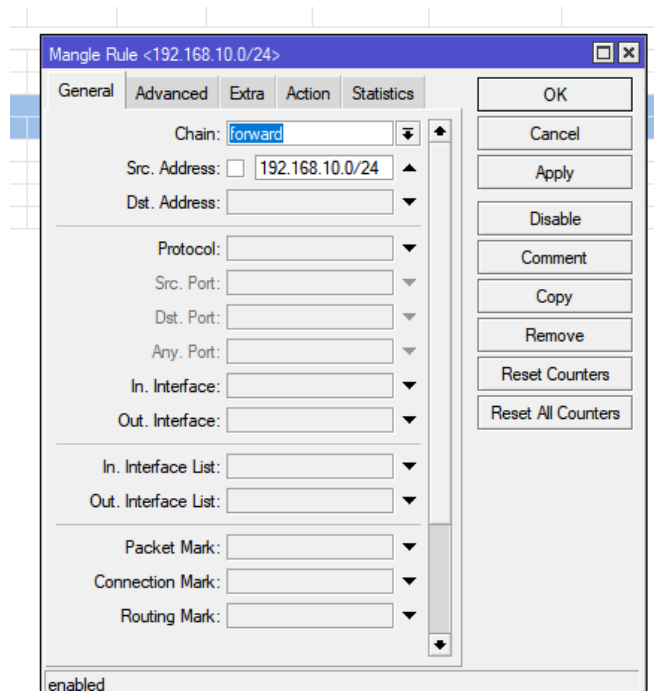
Gambar 3. 94 Tampilan Mangle Packet Sisa Mark Connection General Masukkan
Ip Yang Digunakan Untuk Mengatur Client Pada Jaringan



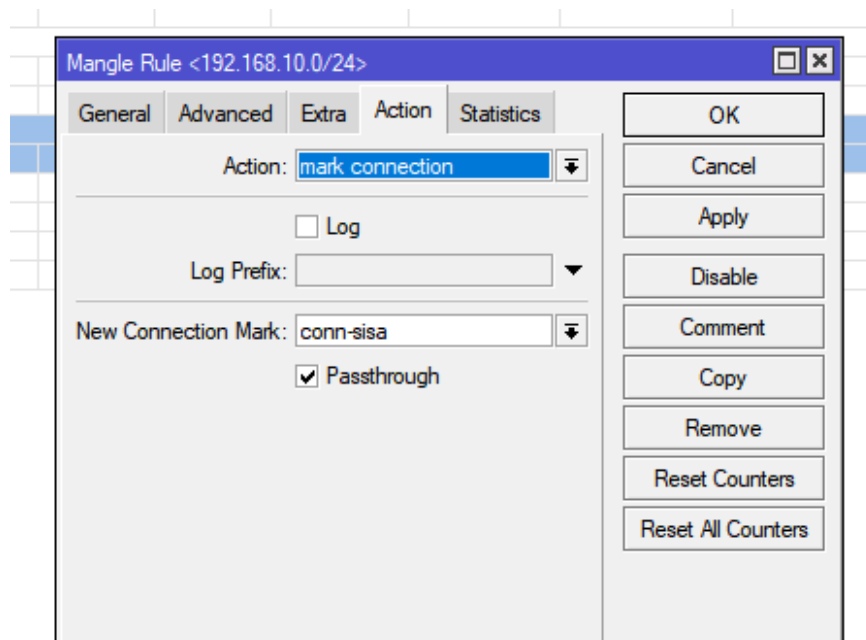
Gambar 3. 95 Tampilan Mangle Packet Sisa Action Mark Connection



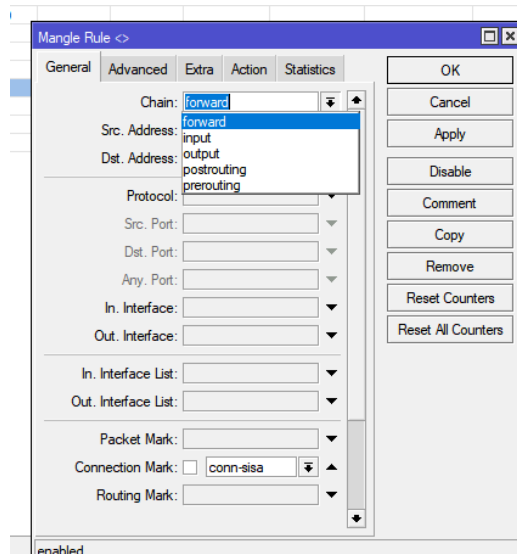
Gambar 3. 96 Tampilan Mangle Packet Sisa Action Conn-Sisa



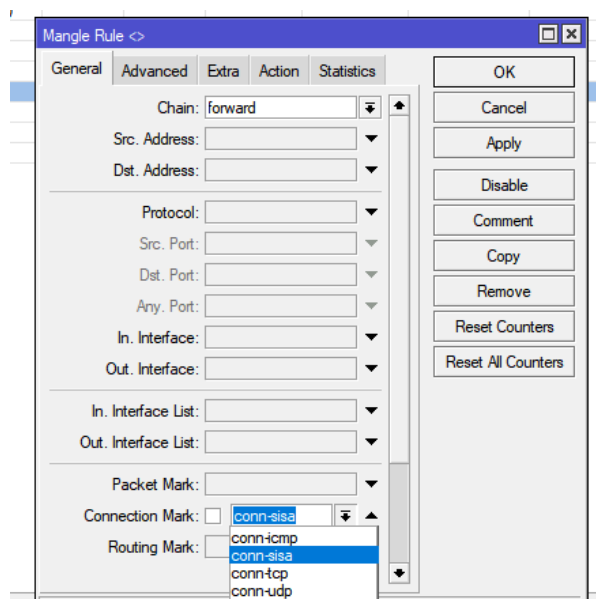
Gambar 3. 97 Tampilan Setting Packet Sisa Mangle Pada Tab General Mark Connection



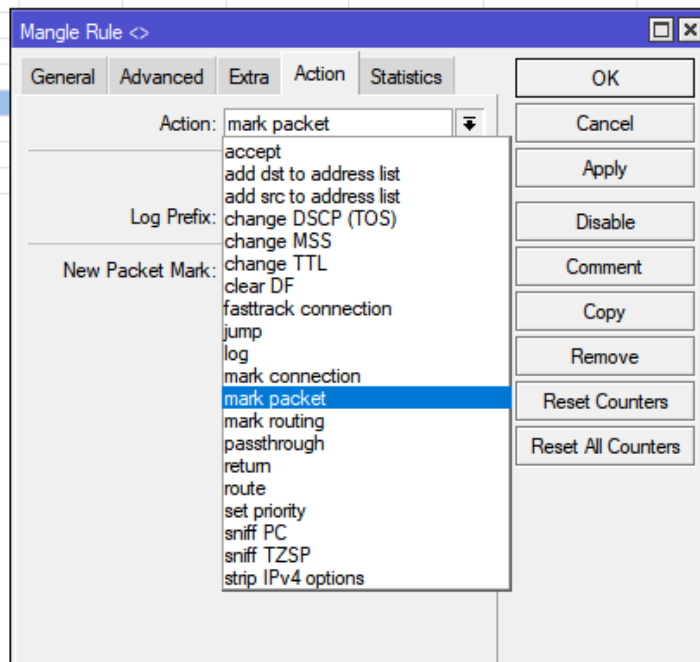
Gambar 3. 98 Tampilan Setting Packet Sisa Mangle Pada Tab Action Mark Connection



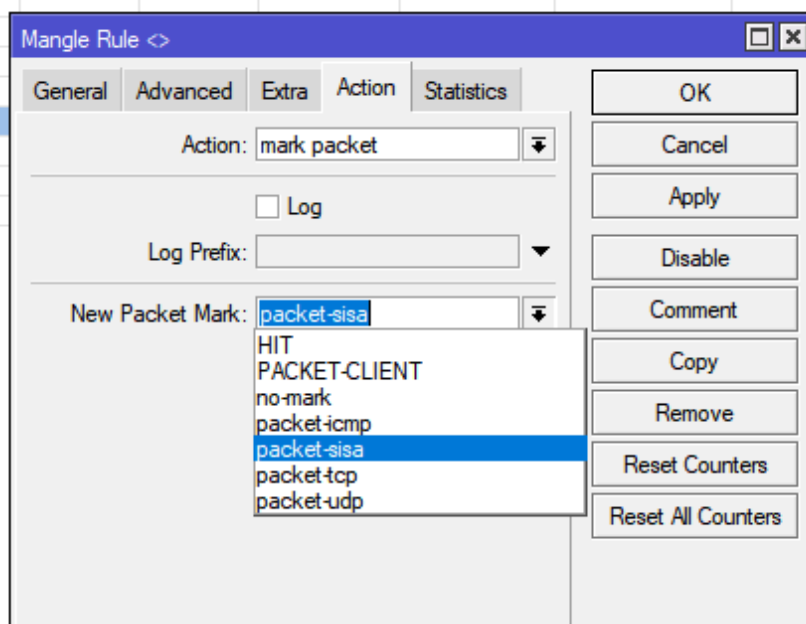
Gambar 3. 99 Tampilan Mangle Packet Sisa Mark Packet General Chain Pilih Forward



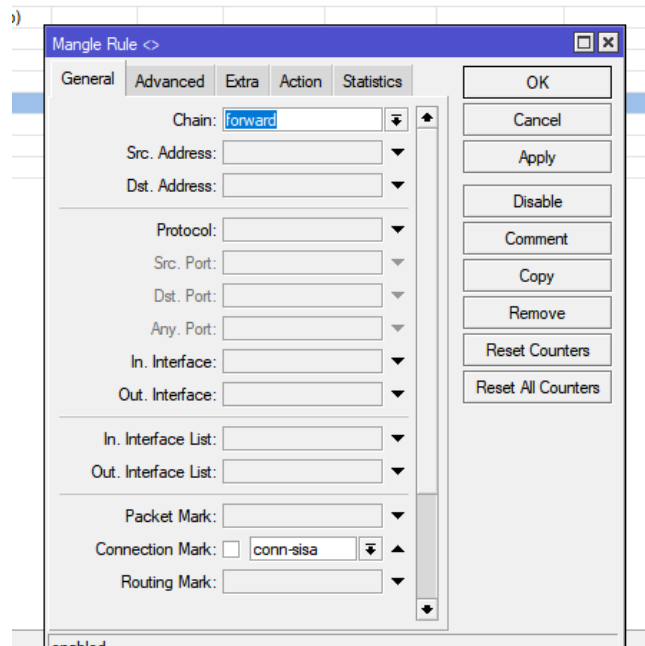
Gambar 3. 100 Tampilan Mangle Packet Sisa Mark Packet General Connection Pilih Conn-Sisa



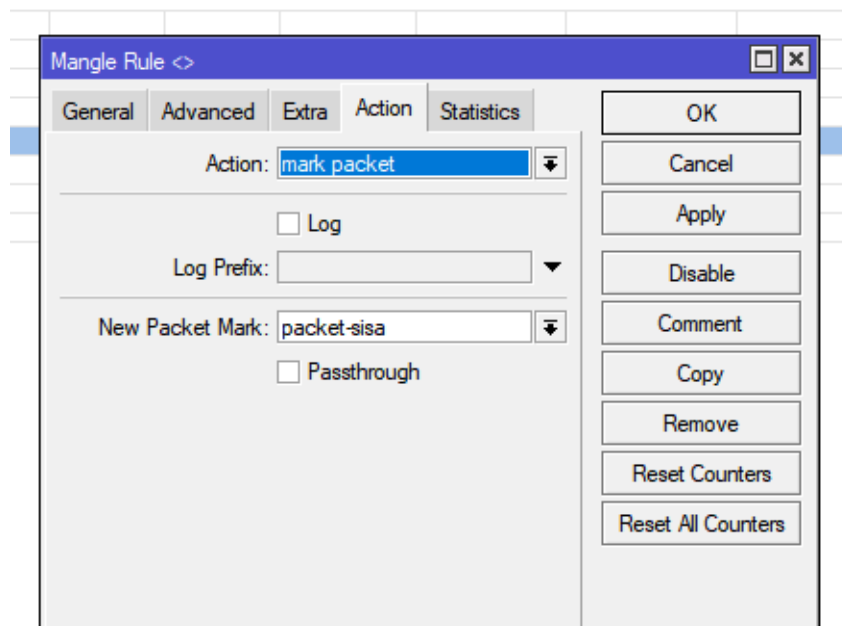
Gambar 3. 101 Tampilan Mangle Packet Sisa Action Mark Packet



Gambar 3. 102 Tampilan Mangle Packet Sisa Action Packet-Sisa



Gambar 3. 103 Tampilan Setting Packet Sisa Mangle Pada Tab General Mark Packet



Gambar 3. 104 Tampilan Setting Packet Icmp Mangle Pada Tab Action Mark Packet

2. QUEUE TREE

Queue tree dilakukan Untuk melihat kumpulan packet yang di upload dan download dapat dilakukan dengan setting sebagai berikut :

Total bandwidth : 400k dengan

Tcp : 150k

Udp : 100 k

Icmp: 50 k

Sisa: 100kbps.

Pengaturan tersebut dapat diterapkan pada Menu queue pilih queue tree.

Buat total bandwidth pada menu add atau pada tanda (+) pilih tab general lalu berikan nama total_download atau sesuai keinginan kemudian buat parent untuk semua download (tcp, udp, icmp, sisa) satu persatu dan arahkan pada total bandwidth pada total download.

Kemudian buat total upload seperti dengan total download dan semuanya pada masing – masing parent berikan limit dan max limit yang tadi sudah diatur total bandwidthnya.

Session: 192.168.10.1

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

00 Reset Counters 00 Reset All Counters Find

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes	Packets
Total Download	ether1			400k	3.4 kbps	0 B	131.1 MB	271 801
Download-ICMP	Total Download	packet-icmp	50k	400k	0 bps	0 B	0 B	0
Download-SISA	Total Download	packet-sisa	100k	400k	0 bps	0 B	0 B	0
Download-TCP	Total Download	packet-tcp	150k	400k	3.4 kbps	0 B	130.4 MB	269 168
Download-UDP	Total Download	packet-udp	100k	400k	0 bps	0 B	888.4 KB	2 778
Total Upload	bridge1			400k	584 bps	0 B	404.2 MB	588 838
Upload-ICMP	Total Upload	packet-icmp	50k	400k	0 bps	0 B	74 B	1
Upload-SISA	Total Upload	packet-sisa	100k	400k	0 bps	0 B	0 B	0
Upload-TCP	Total Upload	packet-tcp	150k	400k	584 bps	0 B	404.2 MB	587 850
Upload-UDP	Total Upload	packet-udp	100k	400k	0 bps	0 B	116.6 KB	1 092

Gambar 3. 105 Tampilan Setting Queue Tree

Dashboard

Session: 192.168.10.1

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

00 Reset Counters 00 Reset All Counters Find

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes	Packets
Total Download	ether1			400k	0 bps	0 B	131.1 MB	271 812
Download-ICMP	Total Download	packet-icmp	50k	400k	0 bps	0 B	0 B	0
Download-SISA	Total Download	packet-sisa	100k	400k	0 bps	0 B	0 B	0
Download-TCP	Total Download	packet-tcp	150k	400k	0 bps	0 B	130.4 MB	269 177
Download-UDP	Total Download	packet-udp	100k	400k	0 bps	0 B	888.5 KB	2 780
Total Upload	bridge1			400k	0 bps	0 B	404.2 MB	588 846
Upload-ICMP	Total Upload	packet-icmp	50k	400k	0 bps	0 B	74 B	1
Upload-SISA	Total Upload	packet-sisa	100k	400k	0 bps	0 B	0 B	0
Upload-TCP	Total Upload	packet-tcp	150k	400k	0 bps	0 B	404.2 MB	587 858
Upload-UDP	Total Upload	packet-udp	100k	400k	0 bps	0 B	116.6 KB	1 092

Queue <Total Download>

General

Name: Total Download

Parent: ether1

Packet Marks:

Queue Type: default

Priority: 8

Bucket Size: 0.100

Limit At: bits/s

Max Limit: 400k bits/s

Burst Limit: bits/s

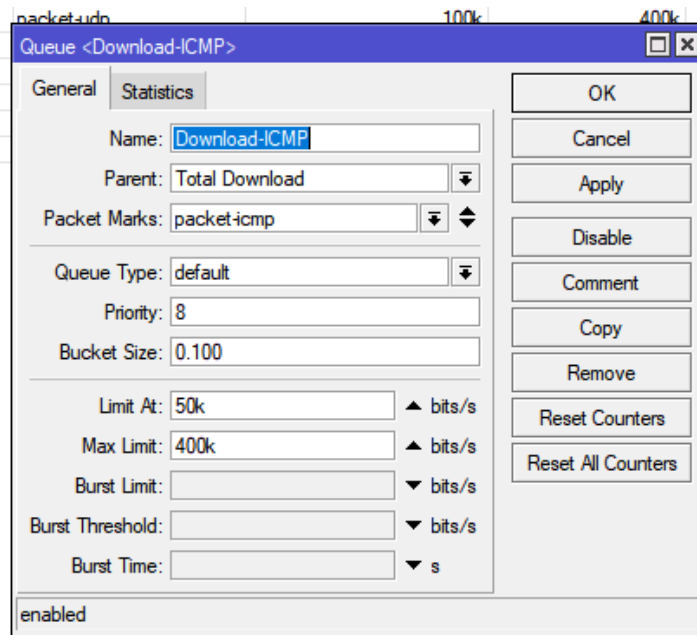
Burst Threshold: bits/s

Burst Time: s

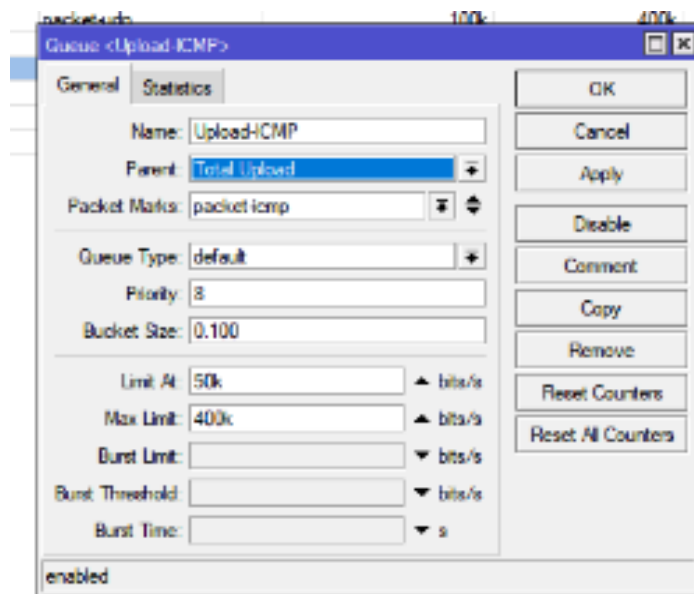
enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

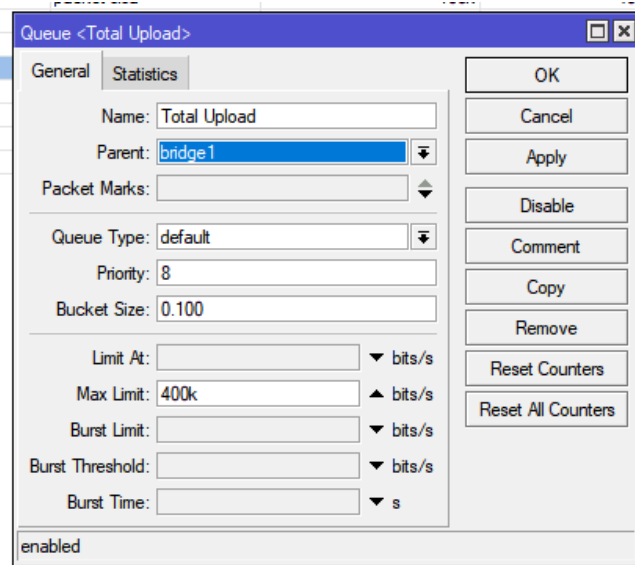
Gambar 3. 106 Tampilan Setting Total Download Pada Queue Tree



Gambar 3. 107 Tampilan Parent Total Download (Icmp Yang Sama Dengan Yang Lain Bedanya Hanya Kapasitas Bandwith Yang Digunakan)



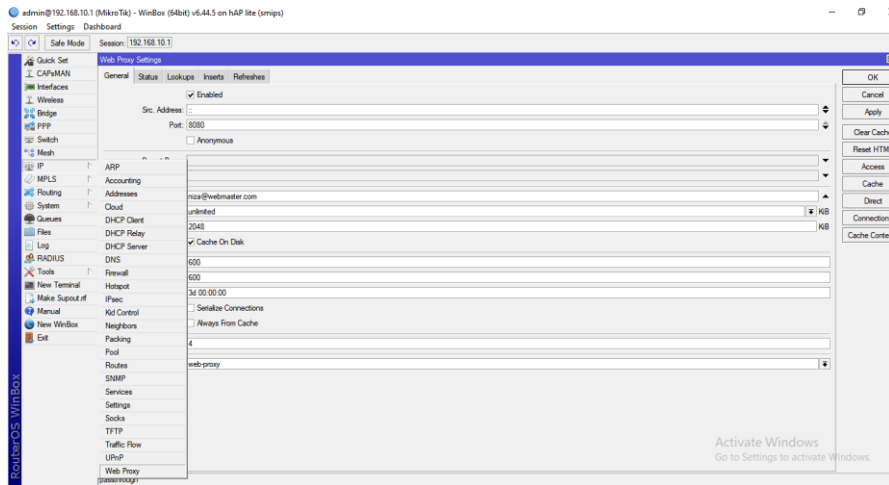
Gambar 3. 108 Tampilan Parent Total Upload (Icmp Yang Sama Dengan Yang Lain Bedanya Hanya Kapasitas Bandwith Yang Digunakan)



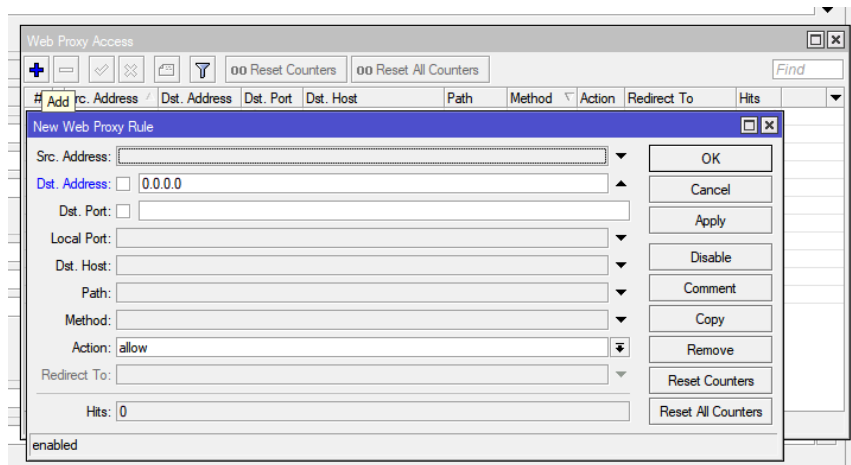
Gambar 3. 109 Tampilan Setting Total Upload Pada Queue Three

1) Setting konfigurasi web proxy mikrotik

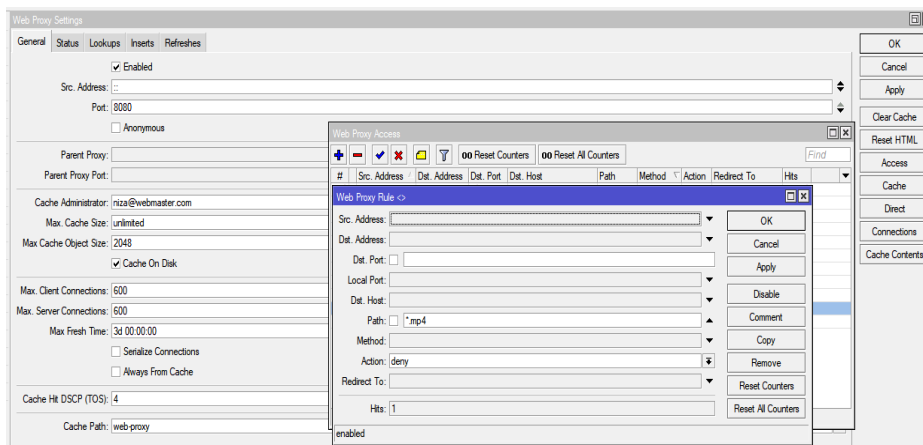
Untuk membuat web proxy pada mikrotik dapat dilakukan pada ip pilih web proxy pada tab general ceklis atau aktifkan enabled isikan port yang ingin dimasukkan tetapi untuk default mikrotik (8080) lalu berikan nama pada cache administrator, ceklis juga pada cache on disk dan masukkan TOS = 4 lalu klik apply dan ok. Buat firewall nat juga untuk meredirect client yang mengakses semua situs. Untuk membuat akses blokir web pada proxy dapat dilakukukan pada menu acces yang ada pada ip web proxy. Untuk melihat cache client yang mengakses atau melakukan aktifitas apapun dapat dibuat pada menu system pilih logging kemudian add atau tambah atau klik tanda (+) dan buat dua log rules pada rules masing masing log memiliki pengaturan yang sama pada menu topics = web proxy dan action = memory dan remote.



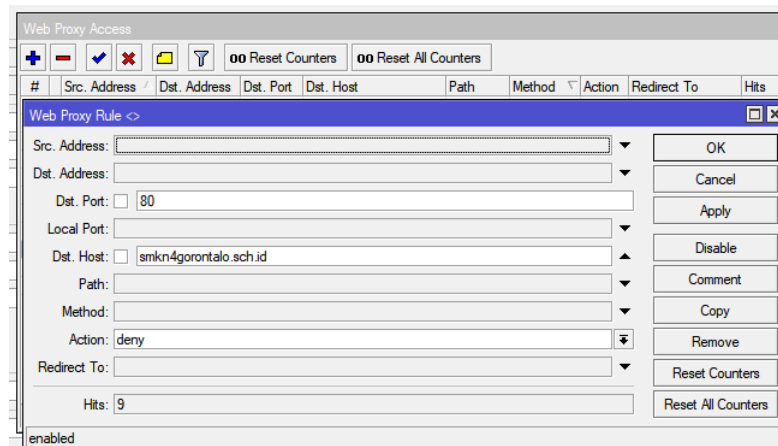
Gambar 3. 110 Tampilan Menu Ip Web Proxy



Gambar 3. 111 Tampilan Setting Blok Akses Pada Web Proxy Mikrotik



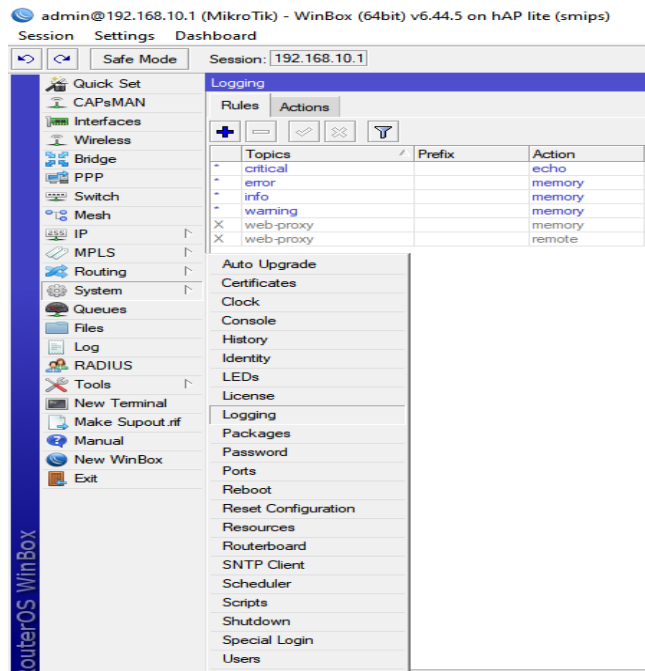
Gambar 3. 112 Tampilan Setting Blok Akses File Mp4 Pada Web Proxy Mikrotik



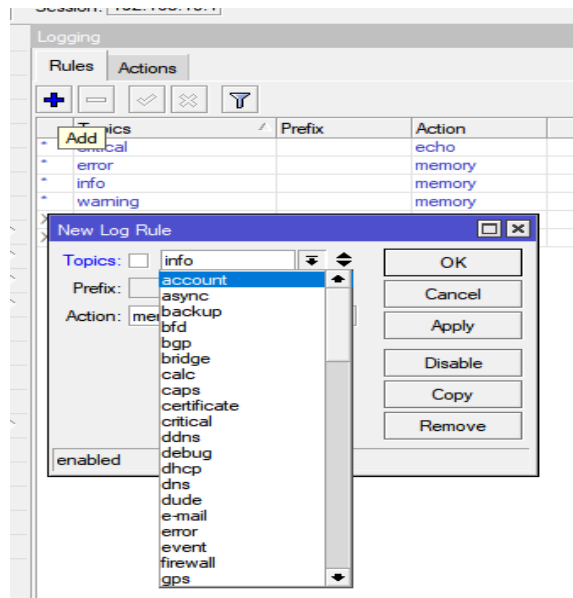
Gambar 3. 113 Tampilan Setting Blok Akses Web (Http) Pada Web Proxy Mikrotik

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To	Hits
0			80	www.google.com			deny		0
1			443	*detik*			deny		0
2			80	smkn4gorontalo.sch.id			deny		0
3				*e-learning.ti.unw.ac.id*			deny		124
4					*.mp3		deny		0
5			80	*youtube*			deny		0
6				*youtube.com			deny	www.google.com	0
7				*siakad.unw.ac.id*			deny		11
8			80	smkn4gorontalo.sch.id			deny		9
9					*.mp4		deny		1
10					*.mkv		deny		2

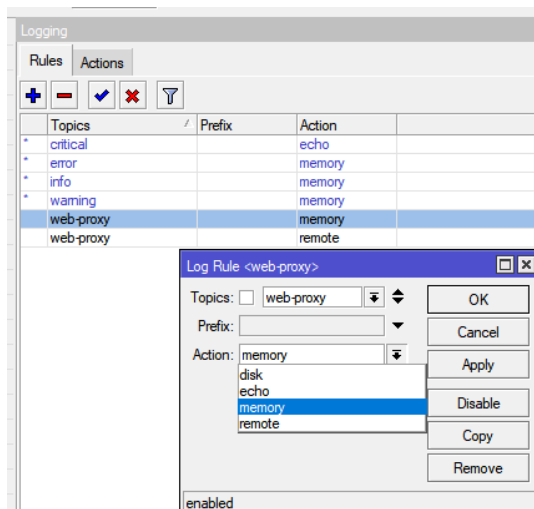
Gambar 3. 114 Tampilan Blok Akses Yang Diterapkan Pada Web Proxy



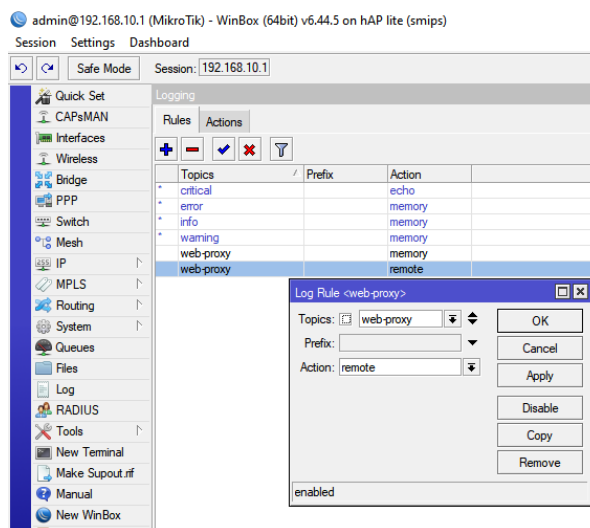
Gambar 3. 115 Tampilan Untuk Mengatur Dan Menampilkan Cache Web Proxy Pada Menu System Pilih Logging



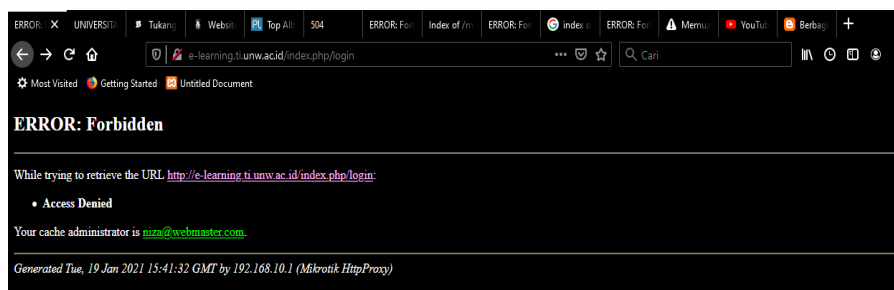
Gambar 3. 116 Tampilan Logging Add Untuk Menambahkan Log Rule



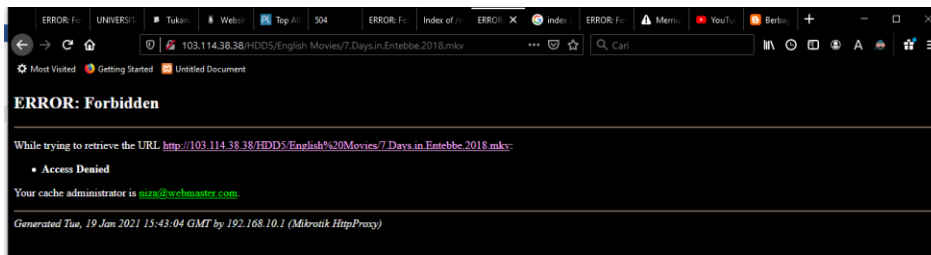
Gambar 3. 117 Tampilan Web-Proxy Pada Log Rules Action Memory



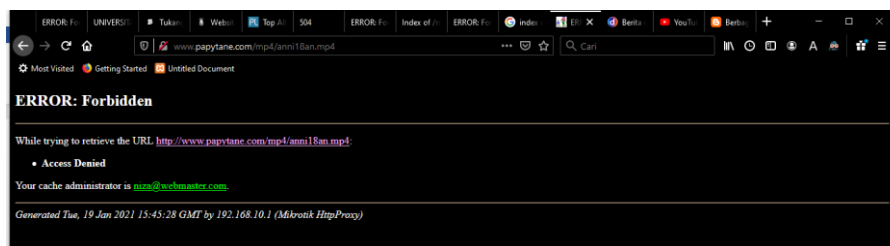
Gambar 3. 118 Tampilan Web-Proxy Pada Log Rules Action Remote



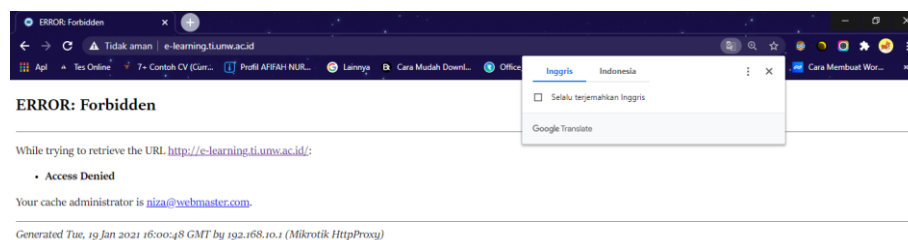
Gambar 3. 119 Tampilan Blok Akses Berhasil Pada Situs Http



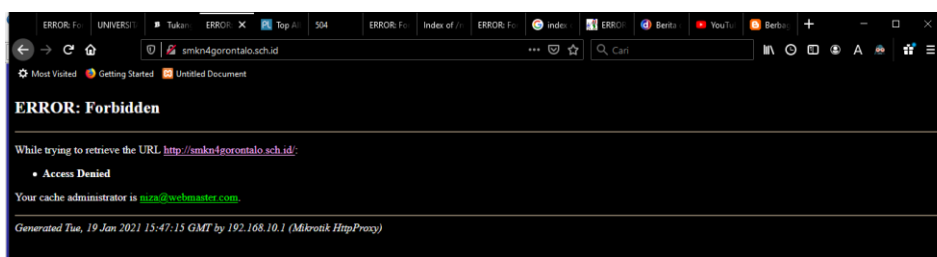
Gambar 3. 120 Blok Akses File Berformat File Video Berformat .Mkv



Gambar 3. 121 Tampilan Blok Akses Berhasil Pada File Berformat Video Mp4



Gambar 3. 122 Tampilan Blok Akses Berhasil Pada Situs Http Dari Browser Lain



Gambar 3. 123 Tampilan Blok Akses Berhasil Pada Situs Http

Session: 192.168.10.1

Log

Freeze

#	Time	Buffer	Topics	Message
431	Jan/19/2021 22:43:49	memory	web-proxy, debug	X-Forwarded-For: 192.168.10.245
432	Jan/19/2021 22:43:49	memory	web-proxy, debug	Via: 1.1 192.168.10.1 (Mikrotik HttpProxy)
433	Jan/19/2021 22:43:49	memory	web-proxy, debug	
434	Jan/19/2021 22:43:55	memory	web-proxy, debug	Response to "GET http://103.114.38.38/HDD5/English%20Movies/null":
435	Jan/19/2021 22:43:55	memory	web-proxy, debug	HTTP/1.1 504 Gateway Timeout
436	Jan/19/2021 22:43:55	memory	web-proxy, debug	Content-Type: text/html
437	Jan/19/2021 22:43:55	memory	web-proxy, debug	Content-Length: 219
438	Jan/19/2021 22:43:55	memory	web-proxy, debug	X-Cnection: Close
439	Jan/19/2021 22:43:55	memory	web-proxy, debug	
440	Jan/19/2021 22:44:03	memory	web-proxy, account	192.168.10.245 GET http://103.114.38.38/HDD5/English%20Movies/null actio...
441	Jan/19/2021 22:44:03	memory	web-proxy, debug	GET /HDD5/English%20Movies/null HTTP/1.1
442	Jan/19/2021 22:44:03	memory	web-proxy, debug	Host: 103.114.38.38
443	Jan/19/2021 22:44:03	memory	web-proxy, debug	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/2010...
444	Jan/19/2021 22:44:03	memory	web-proxy, debug	Accept: */*
445	Jan/19/2021 22:44:03	memory	web-proxy, debug	Accept-Language: id,en-US;q=0.7,en;q=0.3
446	Jan/19/2021 22:44:03	memory	web-proxy, debug	Accept-Encoding: gzip, deflate
447	Jan/19/2021 22:44:03	memory	web-proxy, debug	X-Proxy-ID: 1628763273
448	Jan/19/2021 22:44:03	memory	web-proxy, debug	X-Forwarded-For: 192.168.10.245
449	Jan/19/2021 22:44:03	memory	web-proxy, debug	Via: 1.1 192.168.10.1 (Mikrotik HttpProxy)
450	Jan/19/2021 22:44:03	memory	web-proxy, debug	
451	Jan/19/2021 22:44:03	memory	web-proxy, account	192.168.10.245 GET http://103.114.38.38/HDD5/English%20Movies/null actio...
452	Jan/19/2021 22:44:03	memory	web-proxy, debug	GET /HDD5/English%20Movies/null HTTP/1.1
453	Jan/19/2021 22:44:03	memory	web-proxy, debug	Host: 103.114.38.38
454	Jan/19/2021 22:44:03	memory	web-proxy, debug	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; rv:84.0) Gecko/2010...
455	Jan/19/2021 22:44:03	memory	web-proxy, debug	Accept: */*
456	Jan/19/2021 22:44:03	memory	web-proxy, debug	Accept-Language: id,en-US;q=0.7,en;q=0.3
457	Jan/19/2021 22:44:03	memory	web-proxy, debug	Accept-Encoding: gzip, deflate
458	Jan/19/2021 22:44:03	memory	web-proxy, debug	X-Proxy-ID: 1628763273
459	Jan/19/2021 22:44:03	memory	web-proxy, debug	X-Forwarded-For: 192.168.10.245
460	Jan/19/2021 22:44:03	memory	web-proxy, debug	Via: 1.1 192.168.10.1 (Mikrotik HttpProxy)
461	Jan/19/2021 22:44:03	memory	web-proxy, debug	
462	Jan/19/2021 22:44:04	memory	web-proxy, debug	Response to "GET http://103.114.38.38/HDD5/English%20Movies/null":
463	Jan/19/2021 22:44:04	memory	web-proxy, debug	HTTP/1.1 504 Gateway Timeout
464	Jan/19/2021 22:44:04	memory	web-proxy, debug	Content-Type: text/html
465	Jan/19/2021 22:44:04	memory	web-proxy, debug	Content-Length: 219
466	Jan/19/2021 22:44:04	memory	web-proxy, debug	X-Cnection: Close
467	Jan/19/2021 22:44:04	memory	web-proxy, debug	

468 items

Gambar 3. 124 Tampilan Cache Aktifitas Yang Dikakukan Cliein

Session: 192.168.10.1

Log

Freeze

#	Time	Buffer	Topics	Message
734	Jan/19/2021 22:45:57	memory	web-proxy, debug	Accept-Encoding: gzip, deflate
735	Jan/19/2021 22:45:57	memory	web-proxy, debug	X-Proxy-ID: 1628763273
736	Jan/19/2021 22:45:57	memory	web-proxy, debug	X-Forwarded-For: 192.168.10.245
737	Jan/19/2021 22:45:57	memory	web-proxy, debug	Via: 1.1 192.168.10.1 (Mikrotik HttpProxy)
738	Jan/19/2021 22:45:57	memory	web-proxy, debug	
739	Jan/19/2021 22:45:57	memory	web-proxy, debug	Response to "GET http://www.papytane.com/mp4/null":
740	Jan/19/2021 22:45:57	memory	web-proxy, debug	HTTP/1.1 404 Not Found
741	Jan/19/2021 22:45:57	memory	web-proxy, debug	Date: Tue, 19 Jan 2021 15:45:58 GMT
742	Jan/19/2021 22:45:57	memory	web-proxy, debug	Content-Type: text/html; charset=iso-8859-1
743	Jan/19/2021 22:45:57	memory	web-proxy, debug	Content-Length: 196
744	Jan/19/2021 22:45:57	memory	web-proxy, debug	Server: Apache
745	Jan/19/2021 22:45:57	memory	web-proxy, debug	X-IPLB-Request-ID: 24510B2F-4E86_D5BA2157:0050_6006FEB6_1D9E0:26...
746	Jan/19/2021 22:45:57	memory	web-proxy, debug	X-IPLB-Instance: 29594
747	Jan/19/2021 22:45:57	memory	web-proxy, debug	
748	Jan/19/2021 22:45:58	memory	web-proxy, debug	Response to "GET http://www.papytane.com/mp4/null":
749	Jan/19/2021 22:45:58	memory	web-proxy, debug	HTTP/1.1 404 Not Found
750	Jan/19/2021 22:45:58	memory	web-proxy, debug	Date: Tue, 19 Jan 2021 15:45:58 GMT
751	Jan/19/2021 22:45:58	memory	web-proxy, debug	Content-Type: text/html; charset=iso-8859-1
752	Jan/19/2021 22:45:58	memory	web-proxy, debug	Content-Length: 196
753	Jan/19/2021 22:45:58	memory	web-proxy, debug	Server: Apache
754	Jan/19/2021 22:45:58	memory	web-proxy, debug	X-IPLB-Request-ID: 24510B2F-649E_D5BA2157:0050_6006FEB6_72A2:237C9
755	Jan/19/2021 22:45:58	memory	web-proxy, debug	X-IPLB-Instance: 29603
756	Jan/19/2021 22:45:58	memory	web-proxy, debug	
757	Jan/19/2021 22:46:24	memory	web-proxy, debug	Response to "POST http://su.fv.avast.com/R/A3oKIGFmOWZiMzNkY2RmMDR...
758	Jan/19/2021 22:46:24	memory	web-proxy, debug	HTTP/1.1 504 Gateway Timeout
759	Jan/19/2021 22:46:24	memory	web-proxy, debug	Content-Type: text/html
760	Jan/19/2021 22:46:24	memory	web-proxy, debug	Content-Length: 219
761	Jan/19/2021 22:46:24	memory	web-proxy, debug	X-Cnection: Close
762	Jan/19/2021 22:46:24	memory	web-proxy, debug	
763	Jan/19/2021 22:47:15	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/ action=deny
764	Jan/19/2021 22:47:17	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/favicon.ico action=deny
765	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny
766	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny
767	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny
768	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny
769	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny
770	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny
771	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://smkn4gorontalo.sch.id/null action=deny

772 items

Gambar 3. 125 Tampilan Cache Aktifitas Yang Dikakukan Client

Session: 192.168.10.1

Log

#	Time	Buffer	Topics	Message
768	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://ankn4gorontalo.sch.id/null action=deny
769	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://ankn4gorontalo.sch.id/null action=deny
770	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://ankn4gorontalo.sch.id/null action=deny
771	Jan/19/2021 22:47:18	memory	web-proxy, account	192.168.10.245 GET http://ankn4gorontalo.sch.id/null action=deny
772	Jan/19/2021 22:48:15	memory	web-proxy, account	192.168.10.245 POST http://su.f.avast.com/R/A3oKIGfmOWZMzNkY2RmM...
773	Jan/19/2021 22:48:15	memory	web-proxy, debug	POST /R/A3oKIGfmOWZMzNkY2RmMDRmMm1SNGMyY1WlZM2lyZWFRZ...
774	Jan/19/2021 22:48:15	memory	web-proxy, debug	Host: su.f.avast.com
775	Jan/19/2021 22:48:15	memory	web-proxy, debug	Accept: */*
776	Jan/19/2021 22:48:15	memory	web-proxy, debug	Content-Type: application/octet-stream
777	Jan/19/2021 22:48:15	memory	web-proxy, debug	Pragma: no-cache
778	Jan/19/2021 22:48:15	memory	web-proxy, debug	Content-Length: 195
779	Jan/19/2021 22:48:15	memory	web-proxy, debug	X-Proxy-ID: 1628763273
780	Jan/19/2021 22:48:15	memory	web-proxy, debug	X-Forwarded-For: 192.168.10.245
781	Jan/19/2021 22:48:15	memory	web-proxy, debug	Via: 1.1 192.168.10.1 (Mikrotik HttpProxy)
782	Jan/19/2021 22:48:15	memory	web-proxy, debug	
783	Jan/19/2021 22:48:45	memory	web-proxy, debug	Response to "POST http://su.f.avast.com/R/A3oKIGfmOWZMzNkY2RmMDR...
784	Jan/19/2021 22:48:45	memory	web-proxy, debug	HTTP/1.1 504 Gateway Timeout
785	Jan/19/2021 22:48:46	memory	web-proxy, debug	Content-Type: text/html
786	Jan/19/2021 22:48:46	memory	web-proxy, debug	Content-Length: 219
787	Jan/19/2021 22:48:46	memory	web-proxy, debug	X-Connection: Close
788	Jan/19/2021 22:48:46	memory	web-proxy, debug	
789	Jan/19/2021 22:51:20	memory	web-proxy, account	192.168.10.245 GET http://ncc.avast.com/ncc.bt action=allow cache=MISS
790	Jan/19/2021 22:51:20	memory	web-proxy, debug	GET /ncc.bt HTTP/1.1
791	Jan/19/2021 22:51:20	memory	web-proxy, debug	Host: ncc.avast.com
792	Jan/19/2021 22:51:20	memory	web-proxy, debug	User-Agent: Avast NCC
793	Jan/19/2021 22:51:20	memory	web-proxy, debug	Accept: */*
794	Jan/19/2021 22:51:20	memory	web-proxy, debug	X-Proxy-ID: 1628763273
795	Jan/19/2021 22:51:20	memory	web-proxy, debug	X-Forwarded-For: 192.168.10.245
796	Jan/19/2021 22:51:20	memory	web-proxy, debug	Via: 1.1 192.168.10.1 (Mikrotik HttpProxy)
797	Jan/19/2021 22:51:20	memory	web-proxy, debug	
798	Jan/19/2021 22:51:20	memory	web-proxy, debug	Response to "GET http://ncc.avast.com/ncc.bt":
799	Jan/19/2021 22:51:20	memory	web-proxy, debug	HTTP/1.1 200 OK
800	Jan/19/2021 22:51:20	memory	web-proxy, debug	Content-Type: text/html
801	Jan/19/2021 22:51:20	memory	web-proxy, debug	Content-Length: 26
802	Jan/19/2021 22:51:20	memory	web-proxy, debug	Date: Tue, 19 Jan 2021 15:51:20 GMT
803	Jan/19/2021 22:51:20	memory	web-proxy, debug	
804	Jan/19/2021 22:51:45	memory	web-proxy, account	192.168.10.245 POST http://su.f.avast.com/R/A3oKIGfmOWZMzNkY2RmM...
805	Jan/19/2021 22:51:45	memory	web-proxy, debug	POST /R/A3oKIGfmOWZMzNkY2RmMDRmMm1SNGMyY1WlZM2lyZWFRZ...

827 items

Gambar 3. 126 Tampilan Cache Aktifitas Yang Dikakukan Client

Session: 192.168.10.1

Web Proxy Connections

	Src. Address	Dst. Address	Last Protocol	State	Tx Bytes	Rx Bytes
S	5.45.59.36	192.168.10.245	HTTP/1.1	idle	601 B	316 B
S	36.91.234.17	0.0.0.0	HTTP/1.1	idle	183 B	151 B
S	77.234.45.81	192.168.10.245	HTTP/1.1	idle	601 B	316 B

Gambar 3. 127 Tampilan Koneksi Client

Web Proxy Connections

	Src. Address	Dst. Address	Last Prot...	State	Tx Bytes	Rx Bytes
S	5.45.58.217	0.0.0.0	HTTP/1.1	idle	1202 B	632 B
S	77.234.45.81	192.168.10.245	unknown	rx header	601 B	0 B
S	103.114.38.38	0.0.0.0	HTTP/1.1	idle	690 B	752 B
S	103.114.38.38	0.0.0.0	HTTP/1.1	idle	345 B	436 B
S	103.114.38.38	0.0.0.0	HTTP/1.1	idle	345 B	316 B
C	192.168.10.245	77.234.45.81	HTTP/1.1	rx body	0 B	524 B
S	213.186.33.87	0.0.0.0	HTTP/1.1	idle	1081 B	4855 B
S	213.186.33.87	0.0.0.0	HTTP/1.1	idle	330 B	434 B
S	213.186.33.87	0.0.0.0	HTTP/1.1	idle	330 B	434 B
S	213.186.33.87	0.0.0.0	HTTP/1.1	idle	330 B	433 B
S	213.186.33.87	0.0.0.0	HTTP/1.1	idle	330 B	433 B
S	213.186.33.87	0.0.0.0	HTTP/1.1	idle	330 B	433 B

Gambar 3. 128 Tampilan Koneksi Client