jaringan

by Kda M

Submission date: 16-Jan-2023 04:35AM (UTC-0500)
Submission ID: 1993512449
File name: buku_3_Repaired_Indra_OK.pdf (4.41M)
Word count: 13330
Character count: 76674

JARINGAN KOMPUTER MENGGUNAKAN MIKROTIK

ROUTEROS

Indra Laksmana, Syukriadi,
Romy Aulia, Teddy Yuliswar,
Trinovita Zuhara Jingga

PRAKATA

Bismillahirrahmanirrahim,

Segala puji dan syukur hanya kepada Allah SWT yang telah melimpahkan rahmat dan karunianya sehingga buku ini yang berjudul Jaringan Komputer Menggunakan Mikrotik Router OS telah diselesaikan. Shalawat serta salam semoga tercurah kepada Rasullullah SAW., beserta keluarganya

Penulis mengucapkan banyak terimakasih kepada Segenap Rekan di Program Sarjana Terapan Teknologi Rekayasa Komputer Politeknik Pertanian Negeri Payakumbuh, Jajaran pimpinan, Ditjen Diksi melalui program Matching Fund, PT. Carano Integrasi Teknologi sebagai mitra kegiatan dan semua pihak yang mendukung, terlibat dalam penulisan dan penerbitan buku ini.

Penulis mengharapkan keberlanjutan dari program ini sehingga Ilmu dan Teknologi Informasi dapat tersebar secara terus-menerus demi kemajuan Bangsa dan Negara kita. Kritik dan saran dari pembaca kami harapkan demi kesempurnaan. Pada akhirnya penulis berharap semoga laporan Penelitian ini dapat memberikan manfaat bagi semua. Amiin

Wasalam

DAFTAR ISI

DAFTAR TABEL

BAB I

TCP/IP Review

Pengenalan Mikrotik Router OS dan Router board

A. Sejarah Mikrotik

Mikrotik adalah perusahaan yang didirikan di Riga, yang merupakan ibu kota Republik Latvia, oleh John Tully (CEO) dan Arnis Riekstins. Proyek ini dimulai dengan menggabungkan teknologi Wireless (nirkabel) dan Linux. Mikrotik adalah produsen perangkat lunak dan perangkat keras router.

Proyek ini dmulai tahun 1995 yang bertujuan untuk menciptakan router Nirkabel. Proyek ini awalnya dibuat untuk Perusahaan *Internet Service Provider* (ISP) yang memakai teknologi nirkabel sebagai cara untuk melayani para pelanggan. Mikrotik adalah operasi sistem berbasis Linux yang digunakan untuk melakukan manajemen perangkat penghubung ke internet sehingga memudahkan pengguna untuk menggunakan aplikasi/layanan pada Internet dari perangkat apa pun. Di sini, mikrotik yang bertindak sebagai router jaringan. Motto dari perusahaan ini adalah "*routing the world*", dan prinsipnya adalah membuat teknologi internet lebih murah, lebih cepat, dan lebih terjangkau.

B. Jenis Produk Mikrotik

1. Router OS

   Adalah Sistem Operasi perangkat penghubung jaringan dimana juga dapat digunakan dengan cara mengubah komputer pribadi (PC) menjadi router yang kuat. Perangkat lunak ini berbasis Linux dan diinstal pada PC sebagai sistem operasi, sehingga PC bisa mengerjakan beberapa fungsi di dalamnya, yaitu sebagai router, sebagai bridge, sebagai firewall, dan pengaturan atau manajemen bandwidth, *hotspot* nirkabel / *hotspot* klien, dan berfungsi sebagai pengatur network lainnya. Berfungsi sebagai server untuk klien, sehingga dapat untuk

melakukan routing jaringan, bahkan untuk manajemen jaringan pada ISP dan penyedia hotspot.

2. Routerboard

Routerboard ialah suatu fitur perangkat keras yang dirancang serta dibuat oleh perusahaan Mikrotik dan memakai sistem operasi RouterOS. Routerboard ialah suatu fitur yang memiliki komponen semacam halnya Komputer namun memiliki dimensi yang *compact* seperti *Processor*, Random Access Memory (RAM), Read Only Memory (ROM) serta Flash memory. Router Board mempunyai beberapa tipe arsitektur, tipe interface serta jumlah interface sehingga kita dapat dengan gampang memilih fitur yang cocok dengan kebutuhan. Terdapat sebagian seri Router board yang juga bisa sebagai sumber wifi, sebagai akses poin *nirkabel*, sebagai bridge, dan wds maupun selaku wifi klien. Seperti seri RB411, RB433, RB600. LHG, MantBox, OmniTik dimana sebagian besar ISP wireless memakai routerboard untuk melaksanakan tugas jaringan nirkabelnya baik selaku access point maupun client. Dengan Routerboard, kita bisa melaksanakan tugas suatu router tanpa bergantung pada Komputer/PC, sebab seluruh fungsi pada router telah terdapat dalam Router board. Bila dibanding dengan sebuah personal komputer yang diinstal dengan Sistem operasi RouterOS, router board ini mempunyai ukuran jauh lebih kecil, jauh lebih simpel serta irit listrik karena disebabkan memakai adaptor berdaya kecil.

Gambar 1.1 Routerboard Mikrotik

C. Fitur Pada Mikrotik

Router OS mendukung beragam driver hardware seperti Ethernet, Kartu Nirkabel, V35, ISDN, Penyimpanan USB, Modem USB 5G/4G/3G, E1/T1. Selain itu, Router OS memiliki fitur yang lebih banyak, yaitu:

- Manajemen user (DHCP, hotspot, radius, dll.). User management digunakan untuk mengatur hak akses setiap user yang terdaftar di Mikrotik. Dapat menentukan fitur mana yang dapat dilihat atau dimodifikasi oleh pengguna. Mikrotik memiliki tiga profil utama, read, write dan full. Secara default, Mikrotik menyediakan pengguna default, administrator dengan profil lengkap.
- Routing (RIP, OSPF, BGP, RIPng, OSPF V3). Routing dinamik menghubungkan segmen jaringan lain untuk mengirimkan paket. Memahami perutean itu penting karena memahami dasar-dasar jaringan itu sangat penting.
- Firewall dan NAT berbasis linux. Firewall NAT mengalirkan jaringan internal multipleks dan mengirimkannya kembali ke jaringan yang lebih luas seperti Internet, MAN, dan WAN. Tidak hanya itu, firewall NAT juga mampu mengelompokkan data koneksi yang masuk, sehingga memudahkan untuk memetakan alamat jaringan internal ke alamat jaringan eksternal
- QoS/pembatas bandwidth (berbasis linux). QoS juga dapat digunakan untuk menetapkan pembatasan yang dilihat dari kriteria yang diberikan dan mengurangi lalu lintas yang menguasai semua bandwidth yang ada. Saat tidak menggunakan QoS, lalu lintas akan secara acak mengisi/menggunakan bandwidth yang tersedia.
- VPN dan Tunneling (EoIP, PPTP, L2TP, PPPoE, SSTP, OpenVPN). Atau Tunnel IP adalah saluran komunikasi jaringan Protokol Internet (IP) antara dua network agar bisa transmisi ke jaringan lain dengan mengenkapsulasi paket data.
- Real Time Tool (seperti Torch, watchdog, mac-ping, MRTG, sniffer). Mikrotik Router OS juga menyediakan berbagai tools yang dapat digunakan untuk memonitor jaringan atau router. Biasanya digunakan untuk inspeksi, pemecahan masalah, pemeliharaan, dan pemantauan.

Jenis Mikrotik yang kedua yaitu Routerboard berbeda dengan RouterOS karena Routerboard adalah *hardware*. Mikrotik jenis ini beroperasi pada hardware asli yang diciptakan Mikrotik. Router Board mempunyai ukuran yang kecil dan friendly. Dan sudah terinstall Router OS pada Router board yang dikonfigurasi dengan benar. Router board memiliki komponen dari RAM, ROM, prosesor serta memori. Router board memiliki sistem pengkodean tertentu, seperti Router board tipe RB951, dimana RB berarti Router board, 9 berarti seri , 5 berarti jumlah port, dan 1 berarti jumlah mini PCI/slot nirkabel. Inisial lain di balik jenis Routerboard meliputi:

- U – yakni mempunyai colokan USB
- A – Advanced, biasanya ada diatas lisensi pada level 4
- H – Hight Performance, artinya pada processor memiliki level lebih tinggi
- R – router dilengkapi dengan wireless card yang tertanam.
- G – dilengkapi dengan port Gigabit
- 2^{nD} – artinya mempunyai dual pada channel

Ada beberapa jenis arsitektur yang berbeda untuk Routerboard Mikrotik, tergantung pada perangkat keras dan versi Routerboard. Setiap versi harus menginstal perangkat lunak sistem operasi router yang benar. Berikut adalah arsitektur Mikrotik:

- MIPSBE digunakan untuk CRS series, RB4xx series, RB7xx series, RB9xx series, RB2011 series, SXT, OmniTik, Groove, METAL, SEXTANT
- x86 digunakan untuk PC / X86, RB230 series
- PPC digunakan untuk RB3xx series, RB600 series, RB800 series, dan RB1xxx series
- MIPSLE digunakan untuk RB1xx series, RB5xx series, RB Crossroads
- TILE digunakan untuk CCR series

Tabel 1.2. Arsitektur Mikrotik

RouterOS-mipsle (Mipsle)	Combined package for mipsle (RB100, RB500) (include system, hotspot, wireless, PPP, security, mpls, advanced-tools, Dhcp, routerboard, ipv6, routing)
RouterOS-mipsbe (Mipsbe)	Combined package for mipsbe (RB400) include system, hotspot, wireless, PPP, security, mpls, advanced-tools, Dhcp, routerboard, ipv6, routing)
RouterOS-powerpc (ppc)	Combined package for powerpc (RB300, RB600, RB1000) (includes system, hotspot, wireless, PPP, security, mpls, advanced-tools, Dhcp, routerboard, ipv6, routing)
RouterOS-x86 (x86)	Combined package for x86 (Intel/AMD PC, RB230) include system, hotspot, wireless, PPP, security, mpls, advanced-tools, Dhcp, routerboard, ipv6, routing)
mpls-test (mipsle, mipsbe, ppc, x86)	Multi Protocol Labels Switching support improvements
Routing-test (mipsle, mipsbe, ppc, x86)	Routing protocols (RIP, OSPF, BGP) improvements

D. TCP / IP

Internet Protocol (IP) diartikan sebagai standar yang mengatur atau mengizinkan koneksi, interaksi dan transfer data (koneksi) yang terjadi diantara banyak komputer (minimal dua). Tanggung jawab Protokol Internet adalah sebagai berikut:

- Yaitu untuk mendeteksi konektifitas hardware.
- Untuk Melakukan teknik handshaking.
- Untuk menjalankan bentuk dari karakter koneksi.
- Memulai atau memutuskan pesan/percakapan.
- memformat pesan apa yang akan digunakan.
- Bagaimana jika ada kesalahan pengiriman?

- Menghitung dan menentukan jalur pengiriman.
- mengakhiri sambungan.

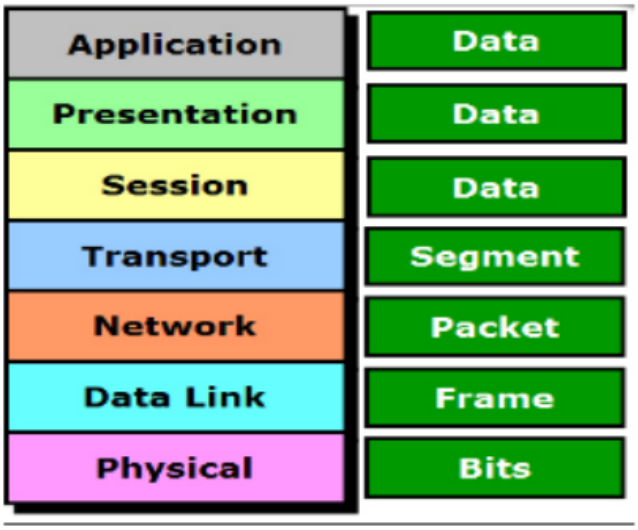
Pada dasarnya, fungsi Internet Protocol atau IP adalah aturan untuk menyambungkan antara pengirim dan penerima untuk komunikasi dan pertukaran informasi, memungkinkannya berfungsi secara akurat. Fitur-fitur lain dari IP, yaitu:

- Enkapsulasi, yaitu informasi yang ingin dikirimkan beserta alamat, kode dari koreksi dan informasi lainnya. Hal tersebut kemudian akan dikirim dalam blog dan dikendalikan oleh unit data protokol. Setiap unit data protokol berisi informasi panggilan dan protokol data sampel dengan kemampuan enkapsulasi, yaitu LLC, ATM, HDLC, IEEE 802.11, IEEE 802.3, AAL5, TFTP, Frame Relay.
- Kontrol koneksi, adalah pembentukan koneksi berkomunikasi antara transistor ke penerima untuk mengirim data dan memutuskan koneksi.
- Kontrol flow, untuk melimit jumlah dari data yang akan dikirim. fungsi Internet Protocol ini harus ada fungsi stop-wait yang berarti setiap PDU diakui terlebih dahulu sebelum kegiatan proses kirim berikutnya dilakukan.
- Error control, yang berfungsi untuk memantau apakah terjadi kesalahan pada saat sedang pengiriman data, sehingga ketika terjadi suatu kesalahan maka paket data langsung dibuang.
- Fragmentasi adalah proses di mana informasi yang diberikan oleh pengirim dikirim ke dalam beberapa paket, dengan urutan beberapa PDU yang mempunyai berbagai batasan ukuran.
- Reassembly adalah mekanisme dimana si penerima mengembalikan paket untuk menjadikannya paket yang lengkap.
- Layanan transport (transmission service), yaitu memberikan layanan berupa komunikasi data mengenai keamanan dan prioritas data. Misalnya, prioritas sebuah paket, mengatur batas koneksi, akses mengenai paket batas kualitas jaringan, dll.

E. OSI Layer Model

Tiadanya aturan baku yang sama membuat banyak perangkat tidak mungkin berkomunikasi satu sama lain, sehingga lapisan OSI (OSI Layer) muncul. Lapisan OSI adalah standarisasi khusus yang menggunakan jaringan sebagai alat komunikasi. Teknologi jaringan yang telah mengalami kemajuan yang pesat dari tahun ke tahun, memungkinkan setiap pengguna (user) di seluruh penjuru dunia dapat berkomunikasi dengan cepat. Organisasi Internasional untuk Standarisasi (ISO) yang berbasis di Eropa mengembangkan model arsitektur jaringan pada tahun 1970 yang disebut Model Referensi OSI untuk Jaringan jenis Terbuka (atau OSI Reference Model for Open Networking). OSI memiliki 7 layer, setiap layer memiliki fungsinya masing-masing. Open Systems Interconnection (OSI) ini yaitu model referensi yang dibuat dari kerangka kerja konseptual. Saat ini telah berkembang dan menjadi standar khusus tentang koneksi.

Tujuan dari lapisan OSI adalah menjadi model referensi bagi setiap vendor atau pengembang, sehingga produk atau perangkat lunak yang dibuat bersifat interpolatif dan pengguna dapat berkolaborasi dengan tanpa penanganan khusus.



Gambar 1.3. OSI Layer

Cara paling mendasar untuk membedakan perangkat komunikasi adalah pada lapisan (layer) 1, Lapisan 2, dan Lapisan 3, karena kita bisa membedakan mana yang Hub atau Bridge, mana yang Switch, atau mana yang Router.

Tabel 1.2 Perbedaan OSI Layer Router, Switch dan Hub

Layer	Nama	Devices	Data Unit	Addressing
Layer 3	Network	Router	Paket	IP Address
Layer 2	Data Link	Switch	Frame	MAC Address
Layer 1	Physical	Hub	Bit	0111001110

Device	Coonectivity	Data Transfer	Memory
Router	Antar Network yang berbeda	Destination IP Address	Routing Table
Switch	Antar Network yang sama	Berdasar MAC Address Tujuan	MAC Address Table
Hub	Antar Network yang sama	Broadcast ke semua port	None

F. Address MAC

Alamat MAC atau *address* MAC singkatan dari Media *Access Control Address* dapat diartikan sebagai alamat pada jaringan di lapisan data link (lapisan 2) pada model lapisan OSI 7 layer. Disini, alamat MAC ditentukan ke kartu jaringan (*Network Interface Card*/NIC). Alamat MAC adalah alamat unik dengan panjang adalah 48 bit yang ditulis menggunakan hexadesimal (0- 9 dan A - F) dan di pisah menjadi 6 kelompok (masing-masing kelompok 8 bit) . Contoh alamat MAC: 02-00-4C-4F-F0-50. Banyak website di internet yang memiliki fitur pengecekan siapa vendor dari Perangkat Jaringan yang kita gunakan, salah satunya macvendor.com.

G. IP Address

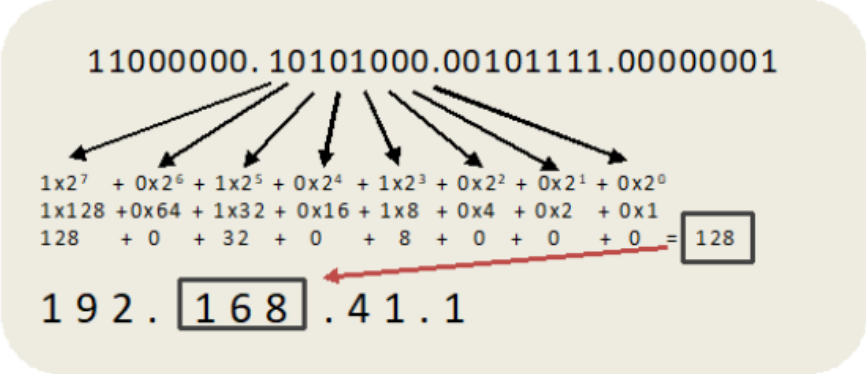
Singkatan dari Internet Protocol, protocol ini bisa ditemukan di lapisan 3 OSI yaitu Network. Alamat IP ini digunakan pada mengalamatkan secara logis PC atau host. Ada dua jenis alamat IP, IPv4 dengan pengalamatan 32-bit hingga 4.294.967.296 host dan IPv6 dengan pengalamatan 128-bit hingga 340,282.366.920.938.463.374.607.431.768.211.456 host.

Ada dua jenis alamat IP yakni IP publik dan kedua adalah IP private. IP publik adalah alamat yang bisa dipakai untuk terhubung langsung ke jaringan internet (global) dan bersifat beda dari yang lain. Sedangkan IP private biasanya dipakai dalam jaringan LAN (lokal). Penetapan IP *private* di tuangkan dalam RFC 1918 dimana rinciannya adalah:

Tabel 1.5. Alokasi IP Privat

RFC1918 name	IP Address range	Number of Address
24-bit block	10.0.0.0 – 10.255.255.255	16.777.216
20-bit block	172.16.0.0 – 172.31.255.255	1.048.576
16-bit block	192.168.0.0 – 192.168.255.255	65.536

Dalam IPv4, dinyatakan dalam notasi menggunakan titik, dibagi menjadi 4 oktal 8 bit. Karena pada tiap oktet adalah 8 bit, rentang nilainya adalah 0 sampai 255 (2^0 s/d 2^7).



Gambar 1.6. sampel pengalamatan Ipv4

H. Subneting

Untuk alamat IP yang dirancang untuk digunakan dalam grup (subnet). Subnetting diartikan sebagi metode untuk memisahkan dan menetapkan beberapa address IP. Host atau perangkat pada subnet yang sama bisa berinteraksi secara langsung antara yang satu yang lain dengan tidak melibatkan router/routing.

Analogi untuk subnet sama dengan path. Jika di satu jalan hanya ada 8 rumah, seorang RT wajib memasang informasi rumah per rumah melalui

jalan tersebut, namun jika jalan tersebut sudah penuh dengan rumah sebaiknya di bagi menjadi beberapa ruas jalan (gang) dan membutuhkan ketua RT di penghujung hari, sehingga meminimalkan lalu lintas saat membuat pengumuman atau informasi dan dapat mengurus setiap rumah di setiap gang/jalan. Subnetting ditulis kedalam 32-bit (seperti alamat IP) atau dalam decimal (prefix).

Contohnya, network 192.168.1.0 mempunyai subnet mask 255.255.255.0 bisa direpresentasikan dalam notasi prefix menjadi 192.168.1.0/24.

Tabel Notasi Subnet

Subnet Mask (Biner)	Subnet Mask (Desimal)	Prefix Length
11111111.00000000.00000000.00000000	255.0.0.0	/8
11111111.11111111.00000000.00000000	255.255.0.0	/16
11111111.11111111.11111111.00000000	255.255.255.0	/24

I. Broadcast dan Network ID

Didalam sebuah grup IP terdapat dua IP khusus, yaitu Network ID yang merupakan identifikasi grup/subnet IP dan broadcast yang merupakan alamat IP yang bisa dipakai untuk memanggil semua address IP dalam grup tersebut. Untuk mendefinisikan network ID dan broadcast address IP dengan subneting tertentu, dapat kita dilakukan dengan menggunakan operasinal gerbang logika AND.

Tabel Contoh Network ID dan Broadcast

Alamat IP	100000011 01101011 10100100 00011010	(131.107.164.026)
Subnet Mask	11111111 11111111 11110000 00000000	(255.255.240.000)
Network ID	10000011 01101011 10100000 00000000	(131.107.160.000)
Broadcast	10000011 01101011 10101111 11111111	(131.107.175.255)

J. Subnetting

Subnetting dapat dijelaskan sebagai proses penguraian atau pembagian jaringan menjadi beberapa jaringan yang lebih kecil. Jenis alamat IP ini biasanya digunakan pada perangkat di jaringan skala lokal (LAN). Semua komputer yang memasuki subnet akan dialamatkan menggunakan bit yang sama, identik, dan paling signifikan yang ditetapkan dalam alamat IP masing-masing. Rumus untuk menghitung subnet adalah $2^{(32-n)}$ yang berarti n = subnet prefix

Tabel Perhitungan Subneting

Prefix	Subnet Mask 255.255.255.(256-jumlah IP)	Jumlah IP	Jumlah Host (Jumlah IP-2)
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.254	2	-
/32	255.255.255.255	1	-

Dalam penentukan range alamat IP, IP host, network ID, broadcast dan subnet mask, misalnya IP address class C: 10.20.20.20/30 dimana kita akan. dapat menggunakan rumus $2^{(32-30)}$ = 22 berarti = 4 untuk melihat banyaknya IP. Cari kelipatan dari jumlah IP (kelipatan 4) : 10.20.20.0 s/d 10.20.20.3 lalu 10.20.20.4 sd 10.20 .20.7, (8-11), (12-15) dan lanjutkan sampai dengan 252-255 untuk range alamat IP. Jadi berada dalam kisaran 10.20.20.20 hingga 10.20.20.23 untuk IPnya. Dari range IP yang ditemukan (10.20.20.20 sampai dengan 10.20.20.23), dimana IP terkecil digunakan untuk network ID, lalu alamat IP terbesar digunakan untuk broadcast network ID 10.20.20.20, broadcast 10.20. 20.23, range IP dikurangi network ID dan IP broadcast host 10.20.20.21 sd 10.20.20.22 (jumlah IP host adalah jumlah IP di subnet

dikurangi 2) dan subnet mask dari 255.255 .255. (256 - jumlah IP) adalah 255.255.255.252 untuk IP klien atau host..

K. Protokol dan Port

Protokol digunakan untuk menentukan proses pengiriman data contoh Transmission Control Protocol (TCP), User Datagram Protocol (UDP) untuk DNS, Internet Control Message Protocol (ICMP) untuk ping traceroute, Hypertext Transfer Protocol (HTTP) untuk Web, Post Office untuk email Protocol (POP3), File Transfer Protocol (FTP), dan Internet Message Access Protocol (IMAP) untuk email adalah protocol yang sering dipakai.

Aplikasi tertentu atau proses perangkat lunak tertentu pada komputer atau host yang menjalankan layanan komunikasi jaringan adalah definisi dari port. 65535 adalah Jumlah total port host, ditentukan nomor dari 0 hingga 1023 (well know port), dari 1024 hingga 49151 (port register), dan untuk port unregister/dinamis, private atau port empheral dari 49152 hingga 65535

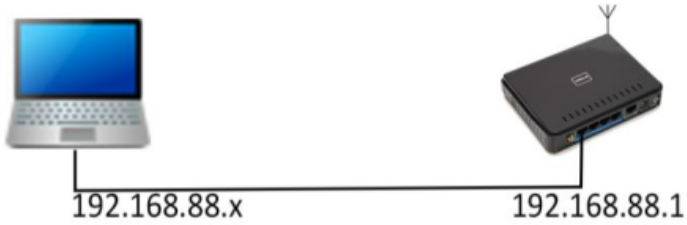
Tabel Penggunaan Port

Port No	Protocol	Service	Remark
21	TCP	FTP	File Transfer Protocol
23	TCP	Telnet	Remote Access
25	TCP	SMTP	Simple Mail Transfer Protocol
53	UDP	DNS	Domain Name Server
80	TCP	HTTP	Hypertext Transfer Protocol
110	TCP	POP3	Post Office Protocol V3
123	UDP	NTP	Network Time Protocol
137	TCP	NetBIOS-ns	NetBIOS-Name Service
161	TCP	SNMP	Simple Network Monitoring Protocol
3128	TCP	HTTP – Proxy	Web-Cache (default by Squid)
8080	TCP	HTTP - Proxy	Web-Cache (customized)

L. Mikrotik Router OS

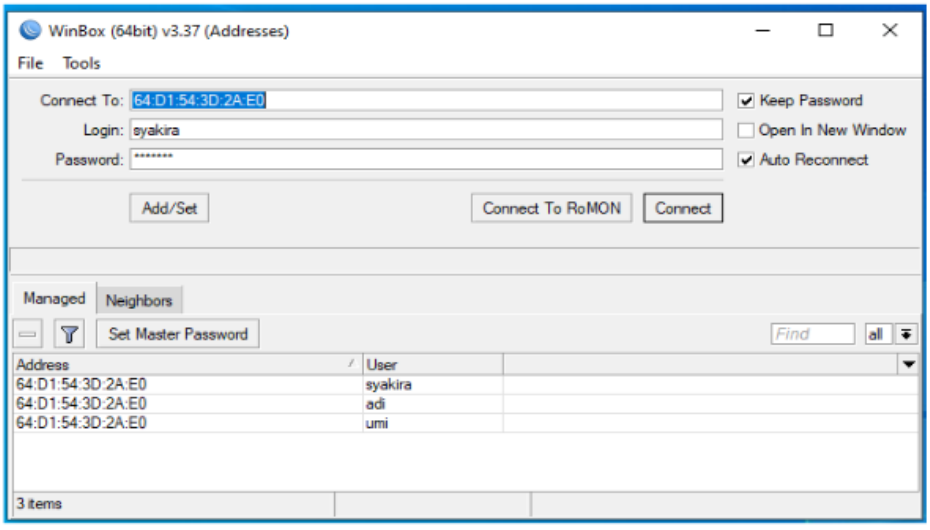
Kita juga dapat mengakses RouterOS pada Routeboard (RB) Mikrotik melalui aplikasi Winbox, yang dapat kita peroleh dari website Mikrotik atau melalui *webfig* IP domain dari router Mikrotik. Pada Router board (RB) baru atau router yang telah direset secara default, konfigurasi defaultnya adalah:

- Alamat IP dari Ether 2-5 : 192.168.88.1/24
- Usernamenya "admin" dan tidak di isi (blank) untuk pasword
- Untuk meremotenya, pada ether1 dan diset dengan IP 192.168.88.xxx/24 untuk PC



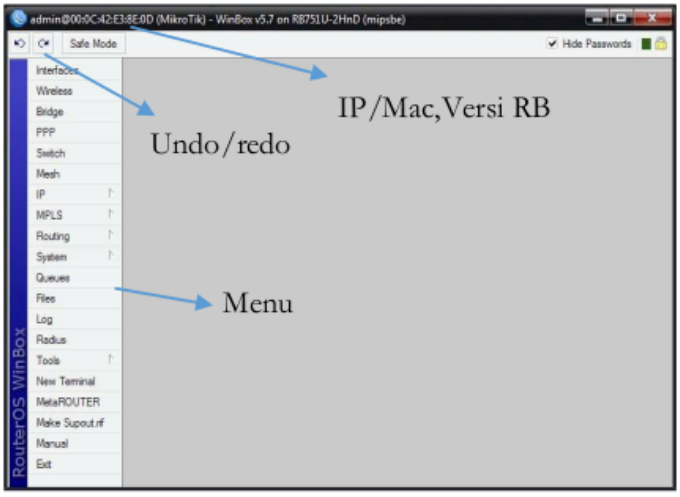
Gambar 1.11. Default Router board

Untuk mengakses RB seperti gambar di atas, pertama-tama kita dapat memodifikasi IP di PC, alamat IP adalah 192.168.88.x, netmask adalah 255.255.255.0, kemudian ping alamat RB sebagai 192.168.88.1, dan akses ke http://192.168 .88.1 di URL. Kita bisa mengunduh winbox disana dan winbox ini adalah cara termudah untuk mengkonfigurasi Mikrotik



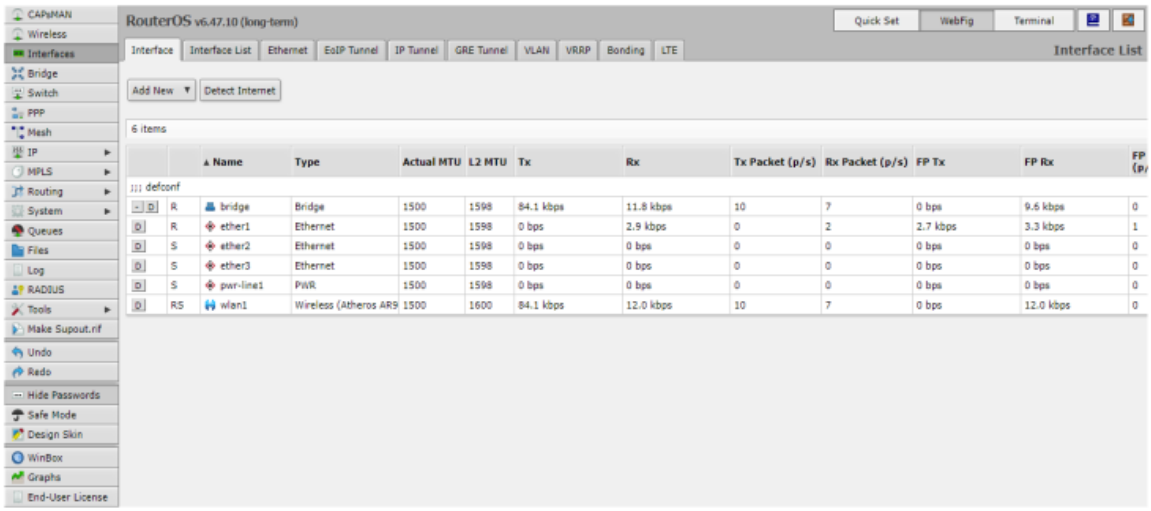
Gambar 1.12. Login Winbox

Setelah login ke winbox, kita dibawa ke halaman utama Mikrotik itu sendiri.



Gambar 1.13. Tampilan Utama Mikrotik di Winbox

Setelah Mikrotik 5.0 dirilis, kini hadir antarmuka (interface) berbasis web dengan fungsi yang sama persis dengan Winbox, aplikasinya bernama Webfig, dimana Webfig menggunakan browser sebagai media untuk mengakses Mikrotik.

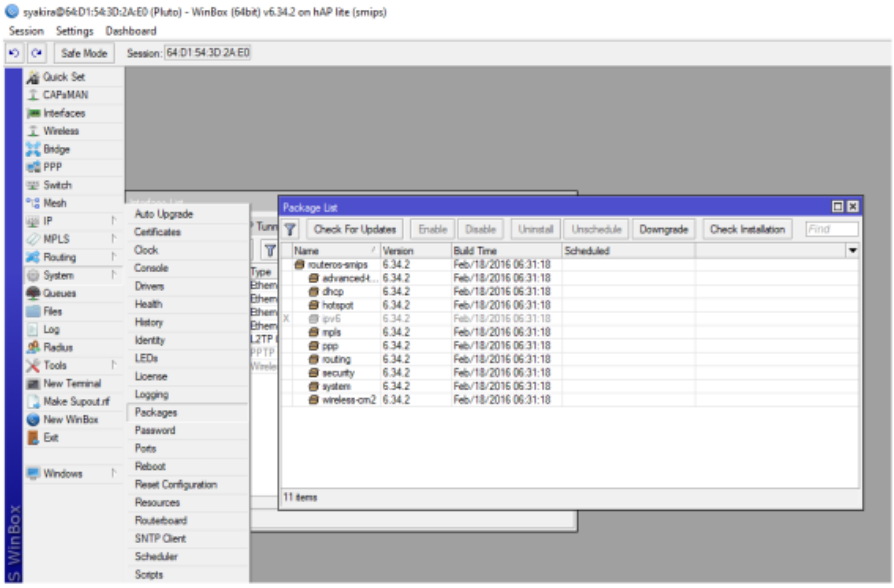


Gambar 1.14. Tampilan Webfig

Selain Winbox, kita juga dapat mengkonfigurasi Mikrotik melalui terminal, akses melalui Telnet (IP port 23, tetapi koneksi tidak aman) atau SSH (IP port 22 dan koneksi yang lebih aman) dan konsol serial (kabel serial). Konfigurasi biasanya dilakukan melalui terminal ketika tidak memungkinkan untuk mengkonfigurasi melalui GUI, seperti bandwidth terbatas, kebutuhan untuk menjalankan skrip, dll. Untuk mengakses Telnet atau program klien SSH/Telnet lainnya seperti menggunakan Putty, WinSCP berbasis prompt MsDOS untuk mengkonfigurasi Mikrotik dari jarak jauh.kita bisa menggunakannya jika kita lupa atau salah menonaktifkan semua interface di Mikrotik atau menggunakan NetInstall atau untuk konsol serial. Untuk operasi jarak jauh melalui konsol serial, kita memerlukan kabel tipe DB-9 (konverter dapat digunakan melalui USB), kemudian gunakan program hyperterminal untuk mengakses

Gambar 1.15. Tampilan via Putty

Fungsional dari Router OS ditentukan oleh tingkat lisensi yang ada pada perangkat. Batasan upgrade untuk paket Mikrotik ditentukan oleh level lisensi. Selain itu, Lisensi ini menentukan berapa banyak versi Mikrotik yang dapat diupgrade pada perangkat keras. Selain itu, fungsionalitas Mikrotik juga tergantung pada versi Mikrotik yang diinstal, yang disertakan dalam Router OS. Paket yangdidukung Router OS dilihat dari Paket yang diinstal. Untuk melihat versi dan paket Mikrotik di Winbox, kita bisa melihatnya dengan memilih menu System -> Packages.



Gambar 1.16. Versi dan Paket Mikrotik

Tabel. Level Lisensi Mikrotik

Level Number	0 (Demo Mode)	1 (Free)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	No Key	Registration Required	Volume only	$45	$95	$250
Upgradable To	-	-	-	ROS V6.x	ROS V7.x	ROS V7.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	Yes	Yes	yes
Wireless Client and Bridge	24h trial	-	Yes	Yes	Yes	yes
RIP, OSPF, BGP Protocol	24h trial	-	Yes (*)	Yes	Yes	yes
EOIP tunnels	24h trial	1	unlimitted	unlimitted	unlimitted	unlimitted
PPPOE Tunnels	24h trial	1	200	200	500	unlimitted

PPTP Tunnels	24h trial	1	200	200	500	unlimitted
L2TP Tunnels	24h trial	1	200	200	500	unlimitted
OVPN Tunnels	24h trial	1	200	200	unlimitted	unlimitted
VLAN Interface	24h trial	1	unlimitted	unlimitted	unlimitted	unlimitted
Hotspot active users	24h trial	1	1	200	500	unlimitted
Radius Client	24h trial	-	Yes	Yes	Yes	Yes
Queues	24h trial	1	unlimitted	unlimitted	unlimitted	unlimitted
Web Proxy	24h trial	-	yes	Yes	Yes	Yes
User Manager Active Sessions	24h trial	1	10	20	50	unlimitted
Number of KVM Guests	None	1	unlimitted	unlimitted	unlimitted	unlimitted

Tabel Fitur Paket Mikrotik

Package	Features
Advanced-tools (mipsle, mipsbe, ppc, x86)	Advanced ping tools, netwatch, ip-scan, sms tool, wake-on-LAN
Calea (mipsle, mipsbe, ppc, x86)	Data gathering tool for specific use due to "communications Assistance for law enforment Act" in USA
DHCP (mipsle, mipsbe, ppc, x86)	Dynamic Host Control Protocol client and server
GPS (mipsle, mipsbe, ppc, x86)	Global Positioning System devices support
Hotspot (mipsle, mipsbe, ppc, x86)	Hotspot user managament
IPV6 (mipsle, mipsbe,	IPV6 addressing support

ppc, x86)	
MPLS (mipsle, mipsbe, ppc, x86)	Multi protocol Label switching support
Multicast (mipsle, mipsbe, ppc, x86)	Protocol Independent Multicast – sparse mode; internet group Managing Protocol - Proxy
ntp (mipsle, mipsbe, ppc, x86)	Network Protocol client and service
ppp (mipsle, mipsbe, ppc, x86)	MIPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP clients and servers
Routerboard (mipsle, mipsbe, ppc, x86)	Accessing and managing RouterBOOT, RouterBOARD specific information
Routing (mipsle, mipsbe, ppc, x86)	Dynamic routing protocols like RIP, BGP, OSPF and routing utilities like BFD, filters for routes
Security (mipsle, mipsbe, ppc, x86)	IPSEC, SSH, Secure Winbox
System (mipsle, mipsbe, ppc, x86)	Basic router features like static routing, ip addresses, SNTP, telnet, APT, queues, firewall, web proxy, DNS cache, TFTP,IP Pool, SNMP, Packet sniffer, e-mail send tool, graphing, bandwith-test, torch, EOIP, IPIP, bridging, VLAN, VRRP etc) Also, for RouterBoard platform – MetaRouter | Virtualization
Ups (mipsle, mipsbe, ppc, x86)	APC UPS
User-manager (mipsle, mipsbe, ppc, x86)	Mikrotik User Manager
Wireless (mipsle, mipsbe, ppc, x86)	Wireless Interface Support

Paket pada Mikrotik dapat diaktifkan, dinonaktifkan, dihapus, diunschedule dan didowngrade. Caranya buka menu package list dan pilih menu action yang akan dilakukan pada paket Mikrotik. Untuk pembaruan dan mendowngrade versi paket, cobalah untuk tetap diperbarui untuk memperbaiki bug dan menambahkan fitur. Downgrade dapat dilakukan jika

perangkat keras tidak mendukung versi baru atau jika ada bug. Untuk pembaharuan, Kita harus mengetahui level dan aturan lisensi Mikrotik kita yang berlaku. Kedua tindakan ini juga harus memperhatikan kompatibilitas jenis arsitektur perangkat keras.

Jika kita lupa username dan password Mikrotik, atau jika kita telah membuat konfigurasi yang sangat kompleks dan perlu diatur ulang, kita perlu mengatur ulang konfigurasi tersebut. Untuk melakukan reset, kita bisa melakukan hard reset pada fisik mikrotik itu sendiri (router board), atau dengan cara soft reset menggunakan software reset atau cara terakhir adalah install ulang. Di Router board, sudah ada tombol reset langsung yang biasanya di belakang perangkat.

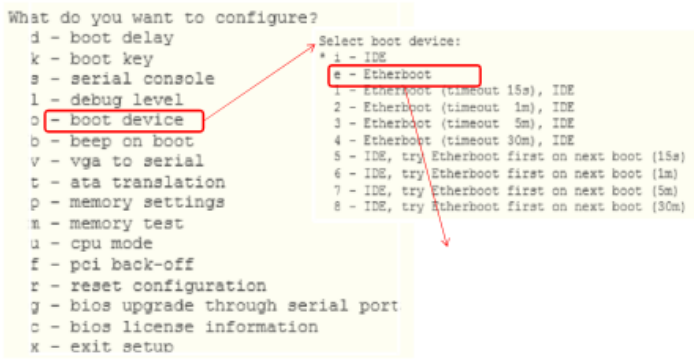
Gambar 1.19. Tombol Reset Router board

Jika kita masih bisa masuk kedalam sistem Mikrotik, maka kita bisa melakukan *soft reset* dengan cara mengetikan perintah pada *command line*, yaitu:

```
[admin@IndraLaksmana] > /system reset-configuration
Dangerous! Reset anyway? [y/N]:
```

Gambar 1.20. Perintah *Soft reset*

Instal ulang diperlukan apabila router kita ingin dikembalikan lagi ke posisi awal / setelan pabrik (*default*). *Software* NetInstall atau install via CD mikrotik bisa kita gunakan untuk install ulang. NetInstall hanya bisa digunakan untuk Router board yang akan diinstall ulang. Posisi RB harus kita seting agar bisa *booting* melalui jaringan (Ethernet card) dengan cara menyeting via *serial console*, menyeting via *terminal console*, menyeting via Winbox dan menekan tombol reset. Agar bisa masuk melalui *serial console* RB melalui NetInstall, kita seting terlebih dahulu dengan cara menekan tombol apa saja di *keyboard* saat tulisan *"Press any key within 2 seconds to enter setup"* terlebih dahulu di BIOS nya

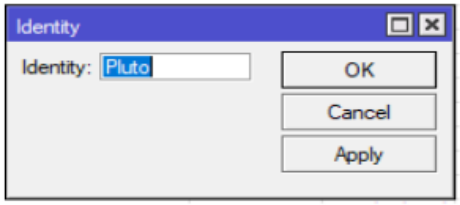


Gambar 1.21. Setingan Booting via *Serial Console*

Jika masih dapat menggunakan Winbox untuk masuk ke sistem, kita dapat memulai Mikrotik dengan membuka menu menu *System -> Routerboard -> Setting -> boot device*. Pilih "*Try-ethernet-once-then-nand*" pada boot device dan OK.

Selain itu, kita dapat menggunakan NetInstall yang berjalan *under* Windows, yang dapat digunakan untuk melakukan instalasi awal dan menginstal ulang Router OS, atau mengatur ulang kata sandi Kita jika Kita lupa. Chek terlebih dahulu PC/Laptop dan harus terhubung langsung ke router melalui kabel UTP dan LAN untuk menjalankannya. NetInstall bisa di download secara resmi dari website Mikrotik. pastikan Laprop/PC kita terhubung ke RB melalui port ether1 dan pastikan sudah bisa "ping" untuk memulainya. Lalu kita bisa merubah perangkat boot RB kita menjadi "*Try-ethernet-once-then-nand*".

Identitas (identity) router sangat diperlukan jika kita ingin membedakan router Mikrotik yang satu dengan yang lainnya, apalagi jika jaringannya kompleks dan besar. Untuk mengubah identitas Kita, Kita dapat masuk ke menu System -> Identity. Identitas router nanti akan terlihat di halaman status Winbox, prompt konsol terminal, penemuan tetangga dan halaman web/webfig



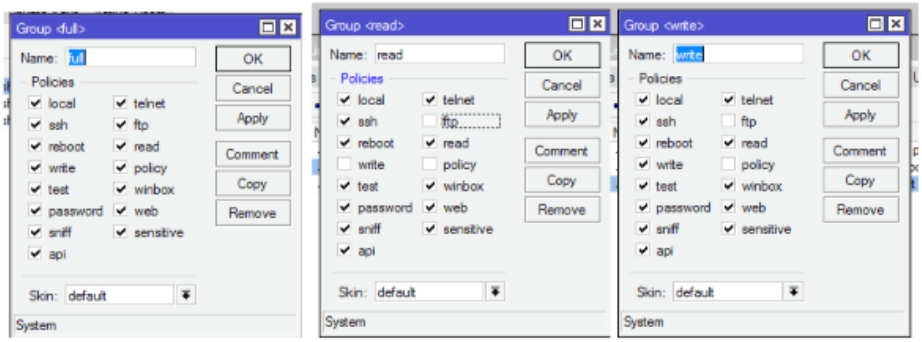
Gambar 1.22. Mengganti Identity

M. User Login Management

Administrator menentukan Siapa yang memiliki akses ke router (menu pengguna). Manajemen pengguna bisa dilakukan seperti cara berikut:

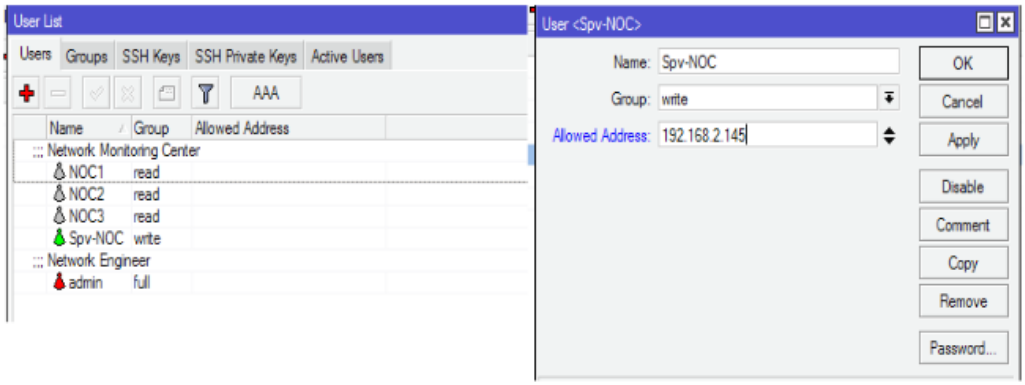
- Grup, digunakan untuk mengelompokkan pengguna, menentukan izin yang dapat diperoleh pengguna.
- User, adalah nama login (username, password) dari seorang user.

Untuk melihat sesi pengguna yang terhubung ke router, Kita dapat melihatnya di *System -> Users -> Active User*. Grup dapat diartikan sebagai cara pengelompokan hak akses yang diberikan kepada pengguna melalui proxy. Ada 3 tipe secara default, yaitu full, read dan write. Kita dapat menyesuaikan hak akses.



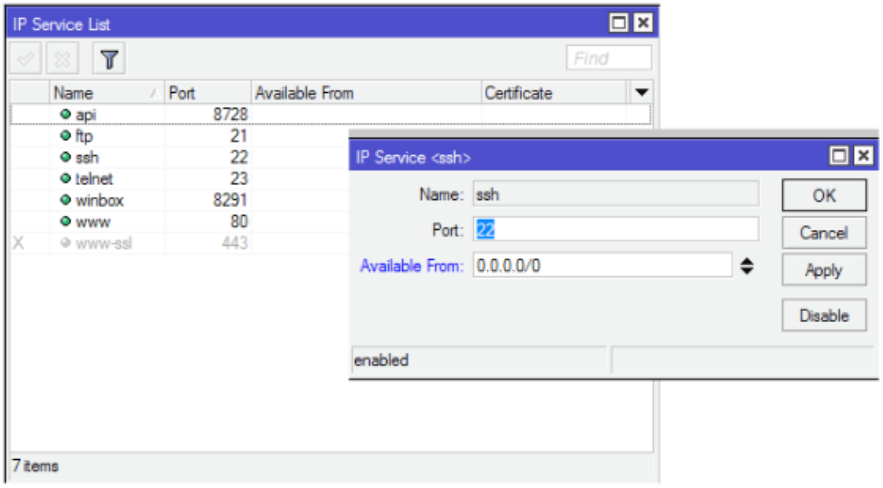
Gambar 1.23. Hak Akses Mikrotik

Setiap pengguna dapat dibatasi hak akses berdasarkan grup, selain itu kita dapat membatasi berdasarkan alamat IP yang digunakan oleh pengguna. Misalnya, PC A mungkin hanya menggunakan alamat IP A atau login hanya dari jaringan A. Daftar pengguna dapat kita lihat pada menu User List.



Gambar.1.24. Hak Akses User List

Layanan (service) perlu dibatasi agar kita dapat menentukan pengguna mana yang dapat mengakses dan dari IP mana mereka dapat mengaksesnya. Untuk mengkonfigurasi layanan ini, kita dapat mengaksesnya melalui menu IP -> Services. Agar lebih aman, kita dapat mengubah port default untuk setiap layanan



Gambar 1.25. IP service List

Selain itu, ada MNDP atau kependekan dari Mikrotik Neighbor Discovery Protocol, yang berfungsi untuk memudahkan kita dalam mengkonfigurasi dan mengelola jaringan kita dengan membiarkan setiap router kita menemukan router lain yang terhubung langsung, dan menemukan router Mikrotik lain yang sedang digunakan. Kemampuannya untuk menemukan router yang menjalankan modul Cisco MNDP dan CDP adalah salah satu kelebihan Mikrotik. Dengan menggunakan aturan filter firewall IP atau menonaktifkan MNDP pada menu IP Neighbor Discovery, kita dapat menyembunyikan Mikrotik kita agar tidak muncul di WInbox saat memindai MNDP.

Setelah dikonfigurasi pada Mikrottik, kita dapat menyimpan konfigurasi untuk digunakan apabila diperlukan nanti. Ada dua jenis backup yang dapat dilakukan, yaitu:

1. Binary File (dengan extensi .backup)

   Jenis cadangan (backup) ini tidak dapat dibaca atau diedit dalam editor teks (misalnya sublime text, dan yang lain). Jenis backup ini bersifat Create Return Point (yang dapat dikembalikan seperti semula) dan mem-backup seluruh konfigurasi Router Mikrotik., Kita bisa menggunakan menu File -> Backup untuk melakukan backup. Untuk mencadangkan konfigurasi router kita yang sebenarnya gunakan tombol backup, dan untuk mengembalikan konfigurasi dari file pilihan kita gunakan tombol restore. Dengan drag and drop sederhana atau FTP untuk menyimpan file di komputer. ini juga Dengan menggunakan terminal, kelebihannya kita bisa menamai file seara bebas sesuka kita untuk Proses backup dan restore binary.

```
[admin@MikroTik A] > system backup save name=bakup_18_nov_11
Saving system configuration
Configuration backup saved
[admin@MikroTik A] > file print
 # NAME            TYPE                                SIZE CREATION-TIME
 0 um-before-mi... .tar file                         16 896 jan/02/1970 07:00:18
 1 skins           directory                                jan/01/1970 07:00:45
 2 MikroTik-181... backup                              25 338 nov/18/2011 13:58:26
 3 MikroTik-020... backup                              15 865 jan/02/1970 07:07:39
 4 bakup_18_nov... backup                              25 338 nov/18/2011 14:10:52
[admin@MikroTik A] >
```

Gambar 1.26. Perintah *Backup* di Terminal

2. Script File (dengan extensi .rsc)

   Jenis skrip ini bisa dibaca dan diedit dalam editor teks. Metode pencadangan ini dapat mencadangkan sebagian atau seluruh konten konfigurasi router. Namun, secara alami Kita tidak dapat mengembalikan konfigurasi seperti sebelumnya, melainkan beberapa skrip harus ditambahkan ke konfigurasi utama Mikrotik. Untuk prosedur pencadangan dan pemulihan mode skrip ini dapat kita lakukan dengan mengeluarkan perintah ekspor (konfigurasi disimpan dengan skrip yang dapat dibaca dan diedit) dan impor (perintah dalam skrip akan dieksekusi). Tujuan dari kedua perintah ini adalah untuk membuat cadangan beberapa konfigurasi dan menjalankannya melalui terminal. Hasil ekspor dapat dilihat pada menu File List.

```
[admin@MikroTik A] > export file=backup-all-config
[admin@MikroTik A] > /ip address export file=backup-ip-config
[admin@MikroTik A] >
```

Gambar 1.27. Perintah Export Scirpt di terminal

```
[admin@IndraLaksmana] > file print
 # NAME                  TYPE                      SIZE CREATION-TIME
 0 bakup_18_nov.backup   backup                 14.3KiB jan/02/1970 00:05:05
 1 labisk.rsc            script                    1119 aug/10/2022 03:57:03
 2 routingmark.rsc       script                    1205 jan/02/1970 00:39:15
 3 basuc-cofig-wirelesi... script                  1281 jan/02/1970 00:03:52
 4 backup-all-config.rsc script                     402 jan/02/1970 00:06:24
 5 backup-ip-config.rsc  script                     127 jan/02/1970 00:08:08
 6 auto-before-reset.ba... backup                20.1KiB jan/01/1970 00:00:06
[admin@IndraLaksmana] > import backup-all-config.rsc

Script file loaded and executed successfully
[admin@IndraLaksmana] >
```

Gambar 1.28. Perintah Import di Terminal

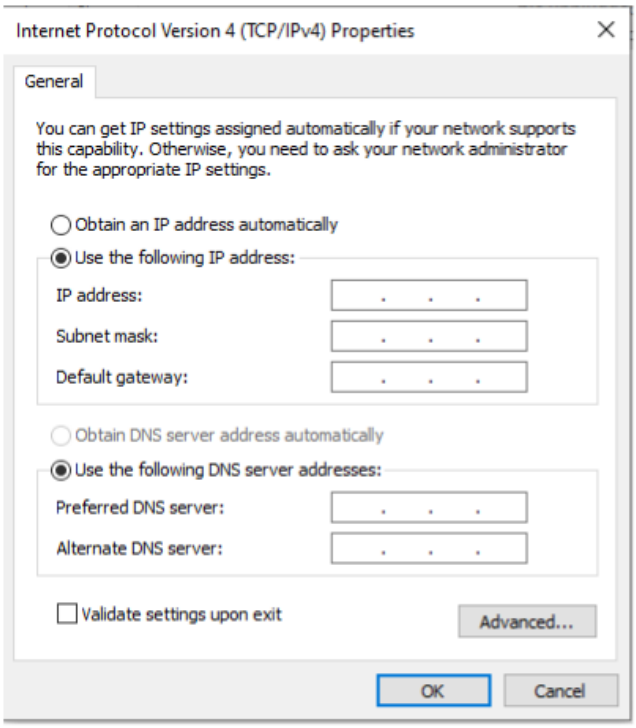
N. Koneksi Internet

Kita bisa menggunakan Mikrotik kita sebagai Network Address Translation atau NAT untuk setup koneksi internet. Untuk terhubung ke router, pertama-tama kita harus mengatur IP kita di Windows/Linux atau sebaliknya.

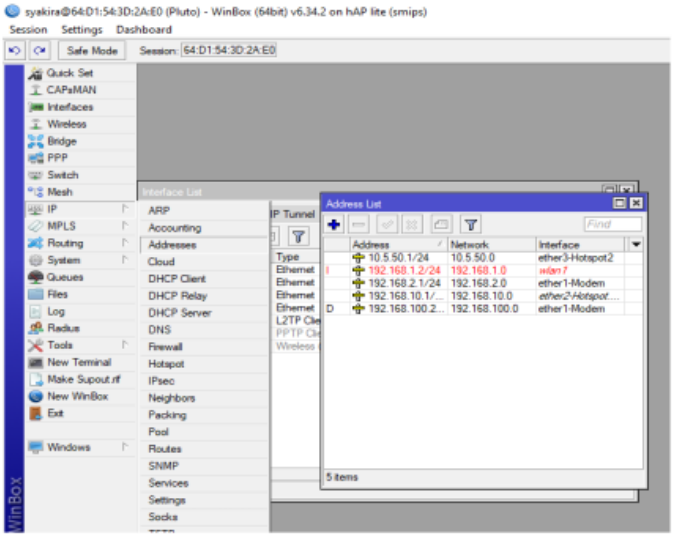

```
[admin@IndraLaksmana] > file print
 # NAME                  TYPE                      SIZE CREATION-TIME
 0 bakup_18_nov.backup   backup                 14.3KiB jan/02/1970 00:05:05
 1 labisk.rsc            script                    1119 aug/10/2022 03:57:03
 2 routingmark.rsc       script                    1205 jan/02/1970 00:39:15
 3 basuc-cofig-wirelesi... script                  1281 jan/02/1970 00:03:52
 4 backup-all-config.rsc script                     402 jan/02/1970 00:06:24
 5 backup-ip-config.rsc  script                     127 jan/02/1970 00:08:08
 6 auto-before-reset.ba... backup                20.1KiB jan/01/1970 00:00:06
[admin@IndraLaksmana] > import backup-all-config.rsc

Script file loaded and executed successfully
[admin@IndraLaksmana] >
```


Gambar 1.29. Simulasi Jaringan Dasar Mikrotik Untuk Koneksi ke Internet

Lalu lakukan setingan IP pada PC/Laptop kita, networknya sama dengan setingan IP pada ether1 Mikrotik (atau ether mana yang terhubung ke laptop / PC)

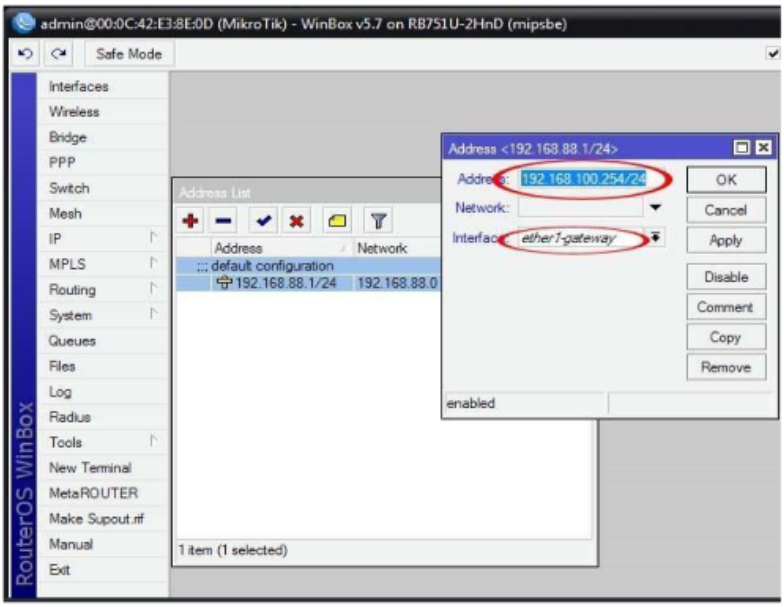


Gambar 1.30. Seting IP Ethernet di PC / Laptop Windows



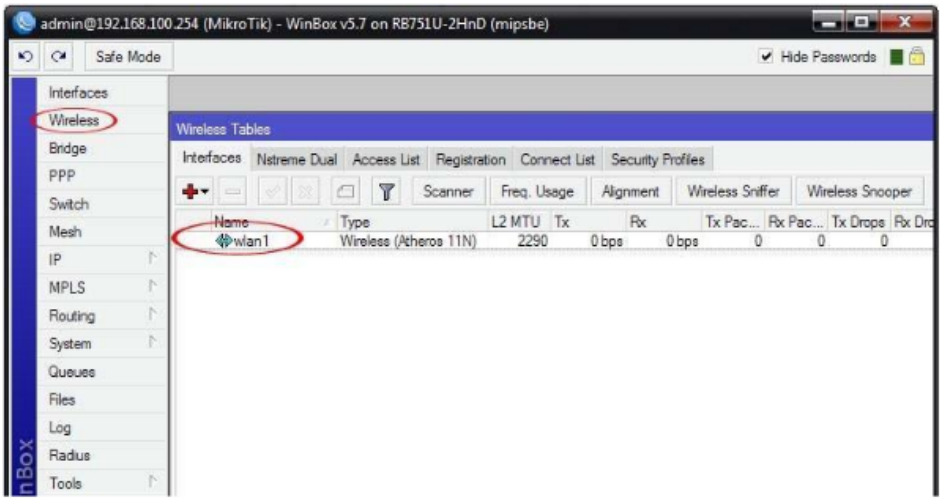
Gambar 1.31. Seting IP Mikrotik yang Ether1 terhubung ke Laptop/ PC

Lalu sesuaikan IP Address Mikrotik kita dengan IP yang kita seting di Laptop atau PC tadi. Lakukan Seting interfacenya ke interface Ether1.



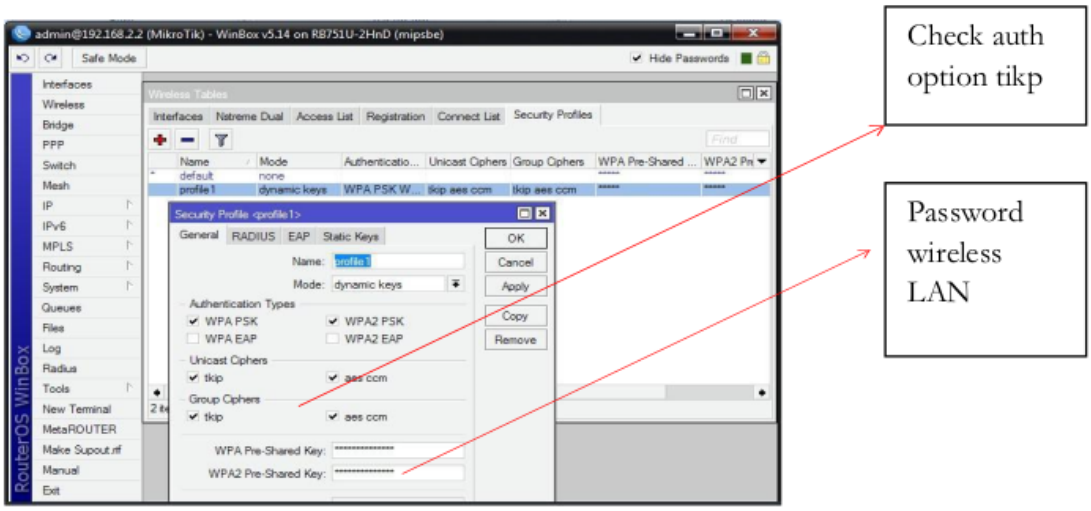
Gambar 1.32. Add IP Adress Mikrotik

Selanjutnya berdasarkan simulasi di atas, kita akan mengkonfigurasi wireless (WAN) pada Mikrotik yang bertindak sebagai sebuah station. Untuk mengkonfigurasinya, kita bisa melalui Wireless -> Interfaces dan klik dua kali pada WLAN1 (pastikan nirkabel kita terdeteksi)..



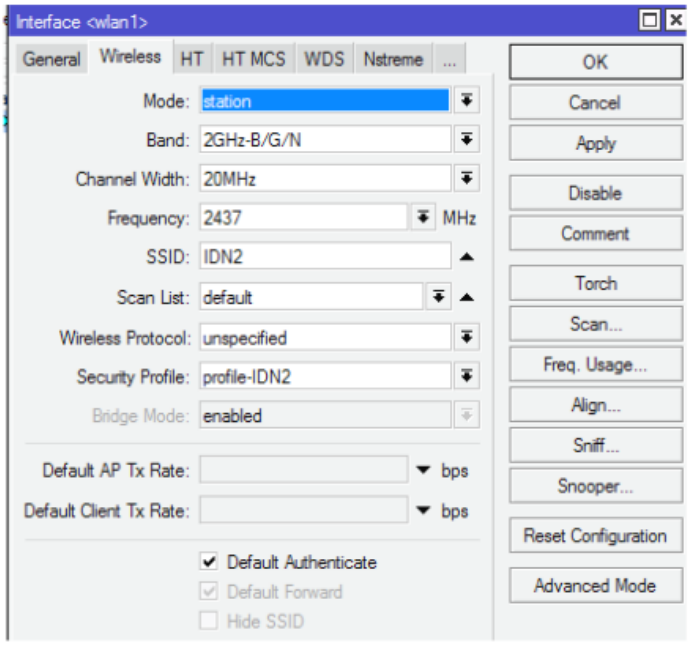
Gambar 1.33. Konfigurasi WLAN Mikrotik

Kemudian selanjutnya kita membuat profil keamanan pada koneksi nirkabel. Fungsinya untuk menambahkan metode otentikasi menggunakan enkripsi key dinamis: WPA/WPA2 dan statis key: WAP

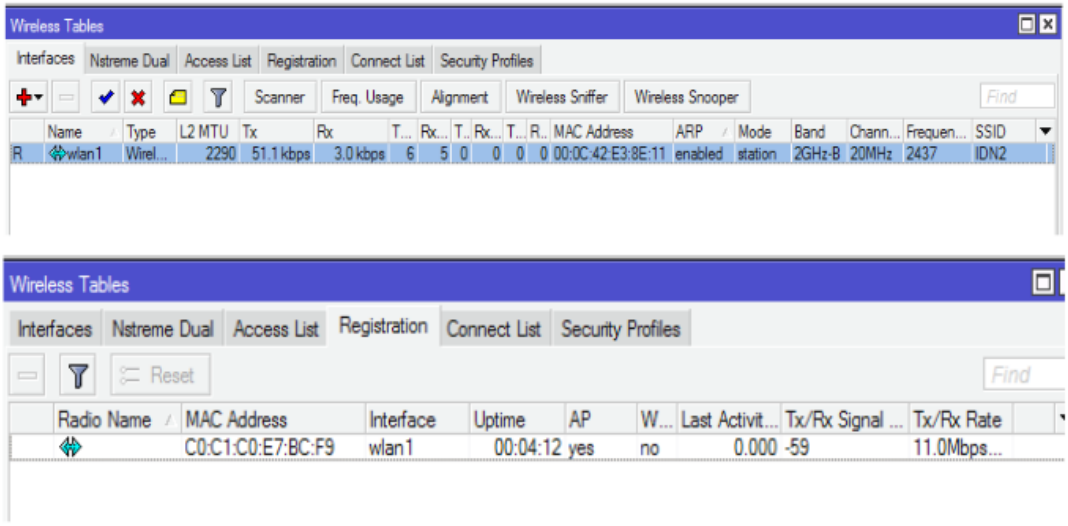


Gambar 1.34. Konfigurasi *security profile* WAN

Masih di bagian Interface pada jendela Wireless Table, kita tetapkan wlan1 sebagai stationnya. Di sini kita mengatur mode wireless, frekuensi, SSID dan profil keamanan. Kita juga bisa menggunakan mode station untuk memindai jaringan agar lebih mudah terhubung ke AP (Access Points). Kita dapat memilih AP yang terhubung dengan memilih tombol hubungkan (connect). Pada menu wireless -> interface dan wireless -> registration kita dapat melihat bahwa nirkabel telah terhubung (tkita R) dan akses poin terhubung.



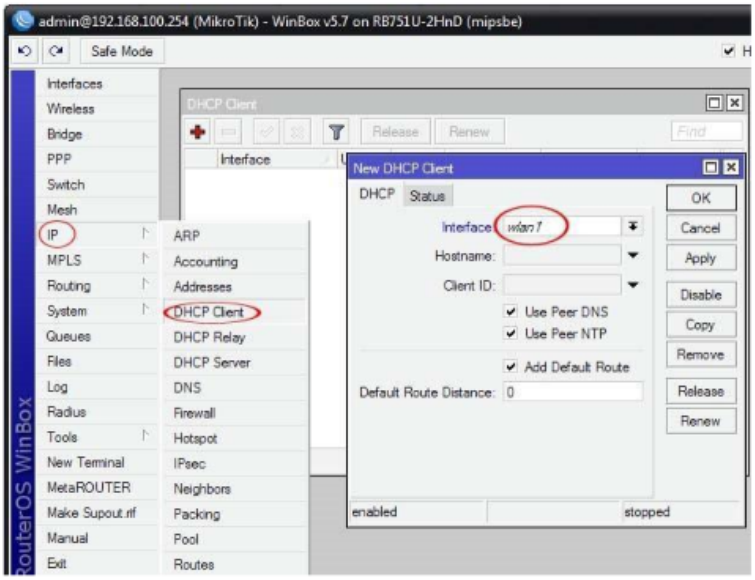
Gambar 1.35. Setting WLAN1 sebagai *station*



Gambar 1.36. Melihat akses poin yang Terkoneksi

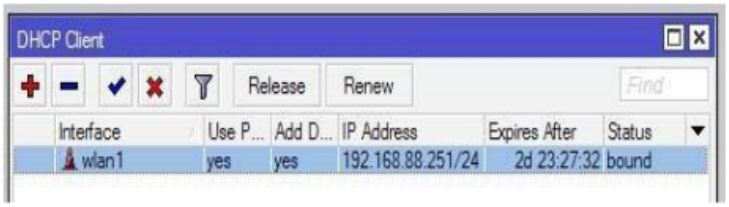
Otomatis pemberikan alamat IP untuk setiap klien yang terhubung ke jaringan computer dilakukan protocol DHCP (Dynamic Host Configuration Protocol) yang memberikan kemudahan bagi administrator mengelola jaringan computer dalam jaringan. Perangkat yang menerima konfigurasi jaringan dari Server DHCP disebut DHCP klien. Biasanya ada banyak perangkat klien dalam jaringan, yang dapat berupa berbagai perangkat. Di Winbox, kita bisa melakukan setting DHCP di menu IP->DHCP Client.

Tetapkan nama antarmuka (interface) DHCP untuk antarmuka WLAN1 dan klik tombol Apply untuk menerapkan konfigurasi.

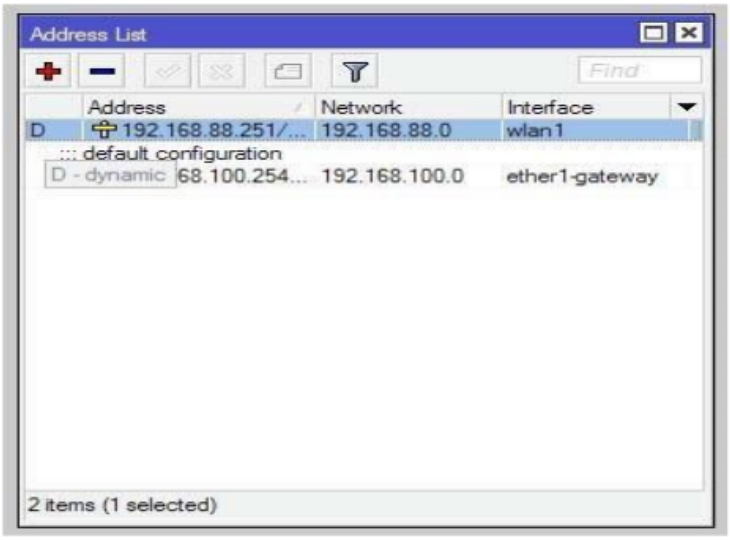


Gambar 1.37. Seting DHCP Client

Nantinya akan terlihat status yang mengatakan jika wlan1 sudah mendapatkan IP address dari AP yang dikoneksikan dengan status *bound* pada setingan DHCP *Client* ini. Jika ingin untuk melihat IP *Address* wlan1 bisa kita lihat pada menu *IP -> Address -> Interface*.

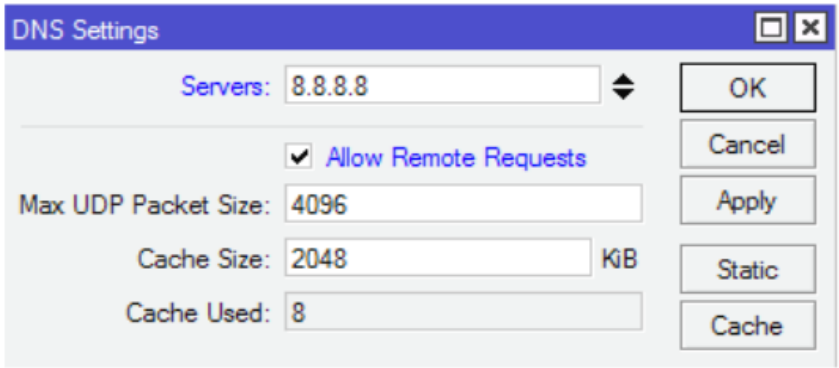


Gambar 1.38. Status Bound

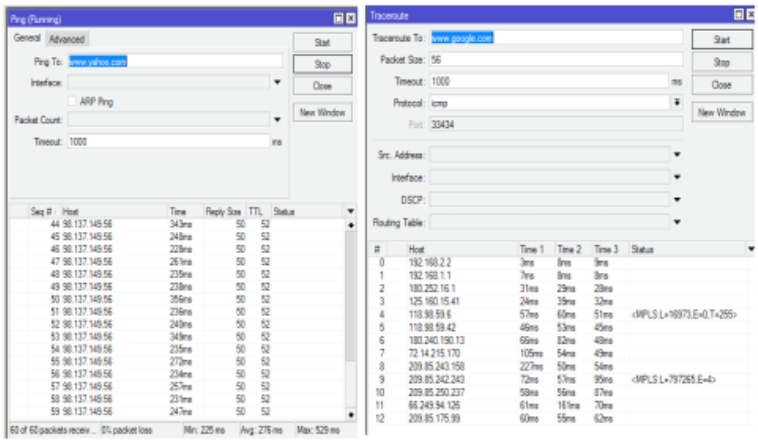


Gambar 1.39. Melihat *Dynamic IP* Wlan

Selanjutnya kita bisa melakukan setting IP DNS. Teknologi yang menerjemahkan domain menjadi alamat IP karena pengalamatan dasar di web menggunakan alamat IP disebut DNS (Domain Name Server). Cara konfigurasi menu IP --> DNS Kemudian pada dynamic server silahkan masukkan IP address DNS server yang kita inginkan, seperti google, cloudflare, OpenDNS, dll. Periksa bagian Allow Remote Requests. Kemudian pilih Terapkan dan OK. Jika sudah, kita bisa mencoba melakukan ping dan tracerouter ke DNS server (misal Google) tadi dengan memilih menu Tools -> Ping and Tools -> Traceroute.

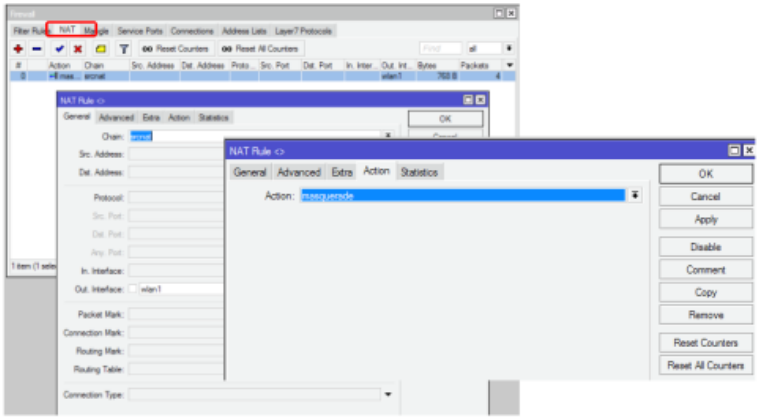


Gambar 1.39. DNS Server Seting



Gambar 1.40. Percobaan *Ping* dan *Traceroute*

Mengkonfigurasi NAT (Network Address Translation) di tahap selanjutnya. Metode menghubungkan beberapa komputer ke Internet menggunakan satu alamat IP disebut NAT. Karena ketersediaan alamat IP yang terbatas makanya metode ini digunakan, selain itu kebutuhan akan keamanan, dan kesederhanaan dan fleksibilitas manajemen jaringan; jaringan yang dirancang untuk menyederhanakan alamat IP dan mengamankan jaringan. NAT adalah teknologi yang memungkinkan jaringan IP *private*, *Router* yang melakukan NAT memungkinkan semua koneksi rumah untuk berbagi satu koneksi Internet melalui satu alamat IP. Untuk mengatur NAT, Kita dapat menggunakan Menu IP -> Firewall -> NAT. Untuk Chain kita bisa mengisinya dengan srcnat, out interfacenya adalah wlan1, pilih masquerade action.



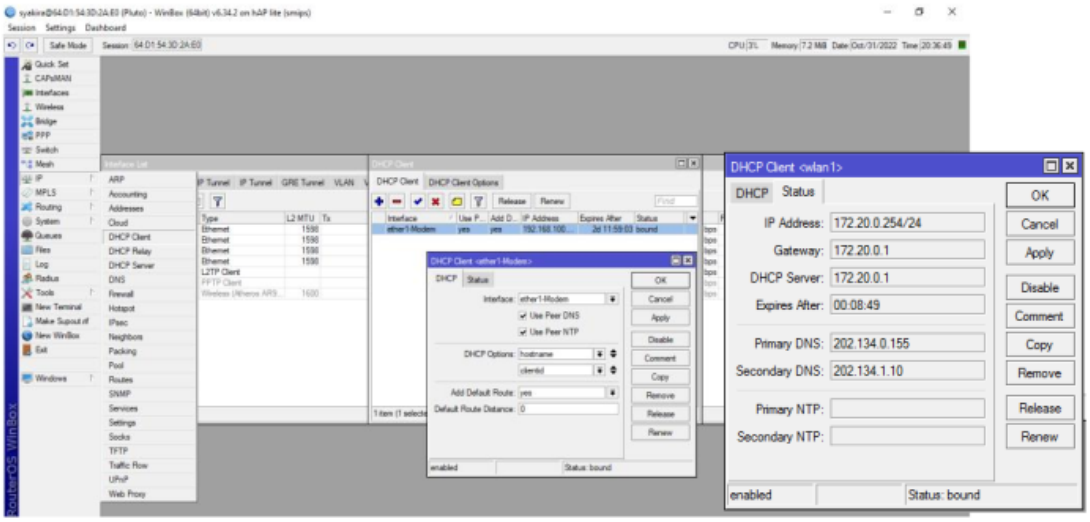
Gambar 1.41. Seting NAT

BAB II
DHCP

Dynamic Host Configuration Protocol adalah singkatan dari DHCP, yang bisa diartikan sebagai protokol untuk menetapkan Konfigurasi jaringan secara otomatis di jaringan lokal. Setiap 1 domain broadcast terdapat satu fungsi DHCP. Fitur DHCP client dan DHCP server didukung oleh Router OS.

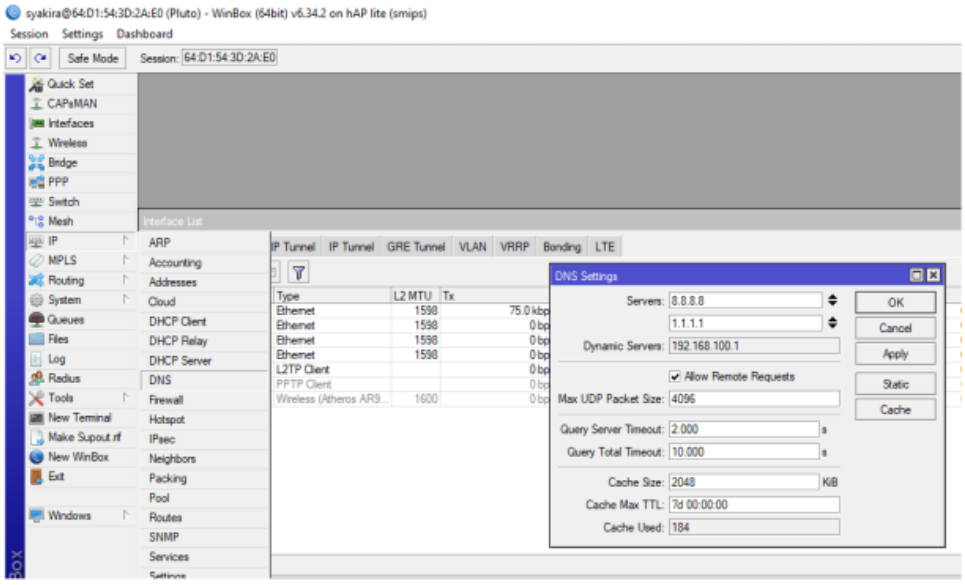
A. DHCP Client

Untuk mendapatkan alamat IP, subnet mask, gateway default, server DNS, dan pengaturan lain yang tersedia secara otomatis digunakan DHCP klien. Router MikroTik memiliki klien DHCP secara default dan dikonfigurasi pada antarmuka ether1 (WAN). Untuk mengkonfigurasi, kita dapat menggunakan Menu IP > DHCP Client > Add. Kita akan menyiapkan klien DHCP pada antarmuka wlan1.



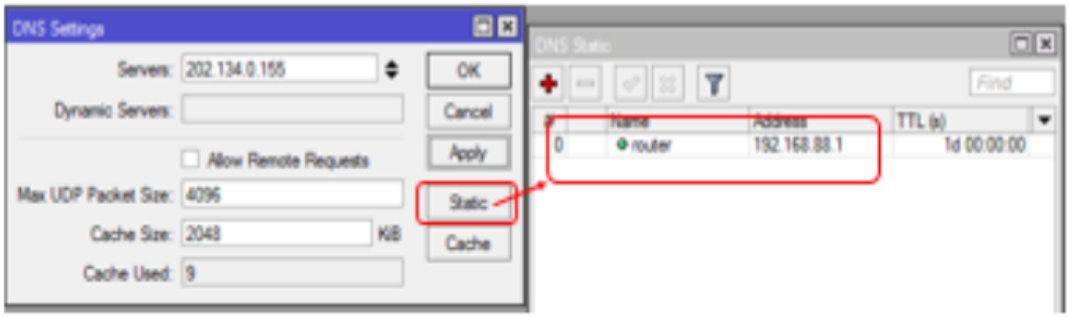
Gambar 2.1. Konfigurasi DHCP Client

Klien DHCP akan meminta alamat IP server DNS. Kita juga dapat mengisi secara manual jika Kita membutuhkan server DNS lain atau DNS tanpa DHCP. Untuk mengaturnya, kita bisa menggunakan menu IP > DNS.



Gambar 2.2. Konfigurasi DNS

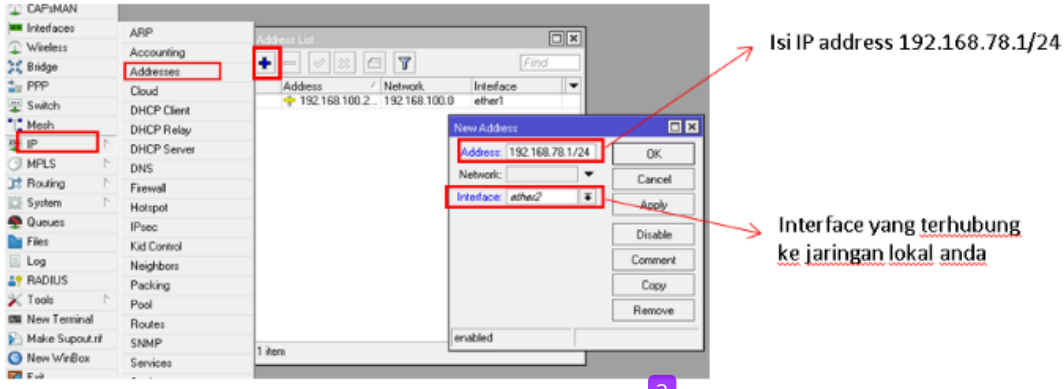
Konfigurasi DNS statis juga bisa dilakukan di Router OS. Secara default, DNS A statis yang disebut router, yang nantinya akan masuk ke 192.168.88.1 (IP router default), yang berarti kita dapat menggunakan nama DNS bukannya IP untuk mengakses router.



Gambar 2.3. Contoh Konfigurasi DNS Static

B. DHCP Server

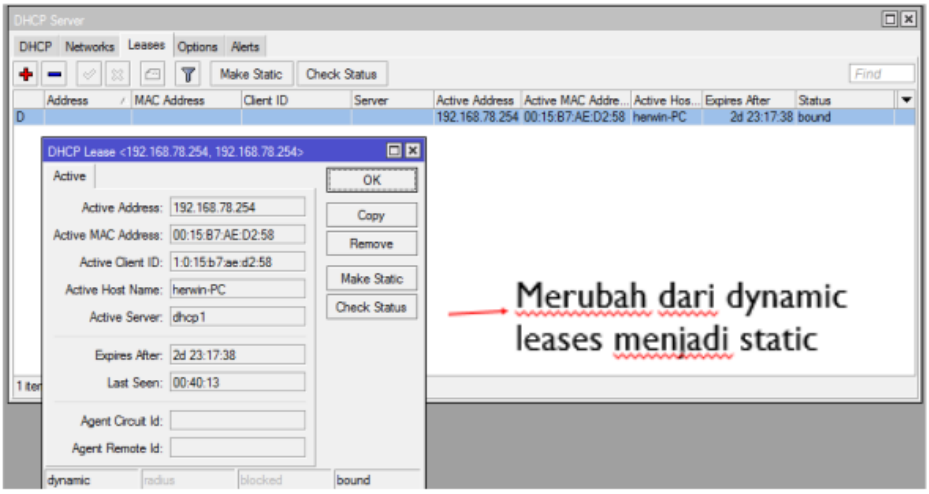
Fungsinya adalah untuk menetapkan konfigurasi jaringan ke host yang memintanya secara otomatis. interface yang akan menggunakan server DHCP nanti harus dikonfirmasi. Kita bisa pakai perintah "DHCP setup" Untuk mengaktifkannya. DHCP server ini dapat berjalan di setiap *interface* router. Untuk memudahkan pengaturan server DHCP, pertama-tama tambahkan alamat IP dari interface antarmuka yang akan menjalankan server DHCP (ini wajib dilakukan sebelum DHCP Server di buat pada Mikrotik RouterOS). Pengaturan server DHCP dapat dilakukan di IP> DHCP Server> DHCP Setup. Setelah server DHCP dibuat, daftar di IP Pool bertambah..



Gambar 2.4. Contoh Konfigurasi DHCP Server

C. DHCP Static Leases

Untuk Menentukan ip yang sama pada perangkat yang sama berdasarkan alamat Mac, digunakan fungsi DHCP Static Lease. Static lease DHCP dapat digunakan tanpa grup IP dan hanya akan mendapatkan alamat yang dikonfigurasi. Kita dapat mengkonfigurasinya pada menu IP > DHCP Server > Leases.



Gambar 2.6. Contoh Konfigurasi DHCP Static Leases

D. ARP

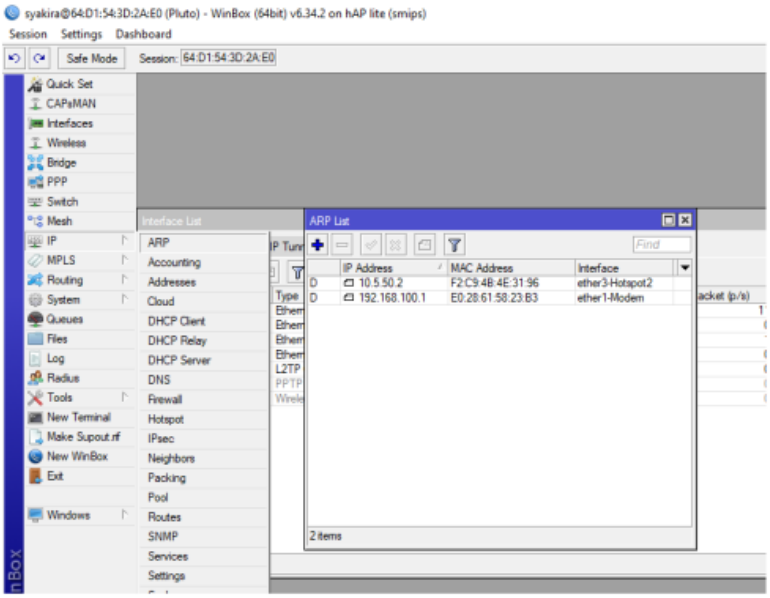
ARP singkatan dari Address Resolution Protocol. Alamat pada perangkat keras harus digunakan untuk mengirimkan host data ke host lain di jaringan yang terhubung meskipun alamat IP digunakan untuk alamat paket atau data. Untuk memetakan layer OSI level 3 (IP) ke OS level 2 (MAC address) adalah fungsi dari ARP ini.

ARP biasanya dibuat secara dinamis oleh router dimana router memiliki fungsi untuk setingan ARP. Konfigurasi untuk ARP juga dapat dibuat sebagian atau seluruhnya secara statis dengan menambahkan ARP secara manual untuk meningkatkan keamanan jaringan. Interface (antarmuka) dalam mode ARP meliputi:

- Enabled: default untuk semua interface di MikroTik dimana Mode ini diaktifkan. Ditemukan dan ditambahkan secara dinamis ke tabel ARP untuk semua ARP.
- Proxy ARP: sebagai ARP proxy transparan antara dirinya sendiri atau jaringan yang terhubung langsung adlah fungsi dari ARP proxy.
- Reply Only: memungkinkan router untuk hanya membalas ARP statis yang ditemukan di tabel ARP, dan akses ke router dan jaringan di belakang router hanya dapat diakses melalui kombinasi alamat IP dan MAC yang ditemukan di tabel ARP adalah fungsi ARP reply-only.

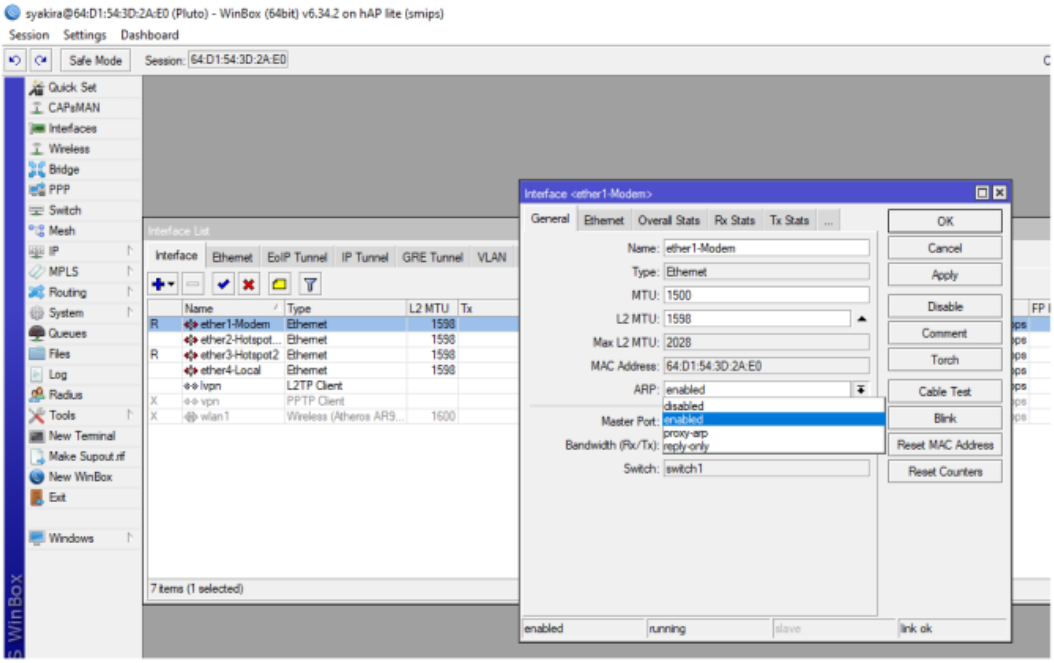
- Disable: entri ARP statis harus ditambahkan di sisi router dan di sisi klien. Misalnya menggunakan perintah arp di Windows: C:\> arp -s 192.168.78.1 00-15-B7-AE-D2-58 jika router tidak menanggapi permintaan ARP klien.

Kita bisa melihat informasi IP, MAC Address dan interface yang tersambung dan terhubung pada ARP table.



Gambar 2.7. ARP list

Kita set interfacenya di *reply-only* dan coba kita akan coba ping dari klient ke router untuk membuat koneksi ARP mode reply only.

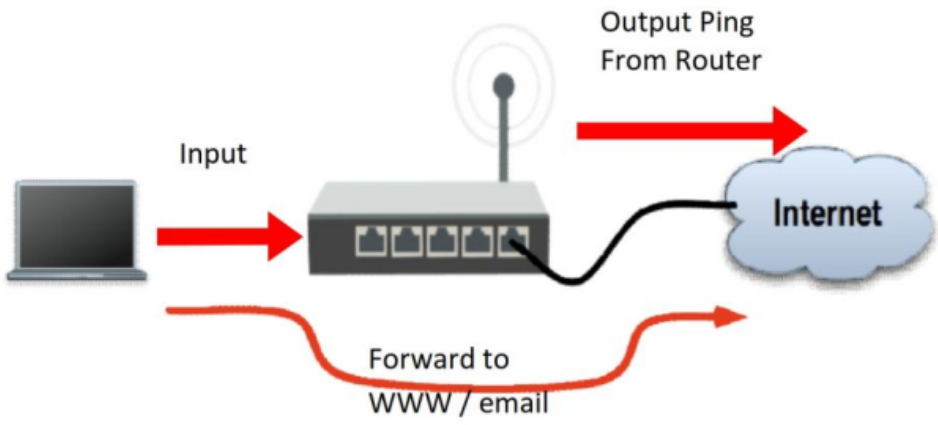


Gambar 2.8. Seting ARP Mode Reply Only

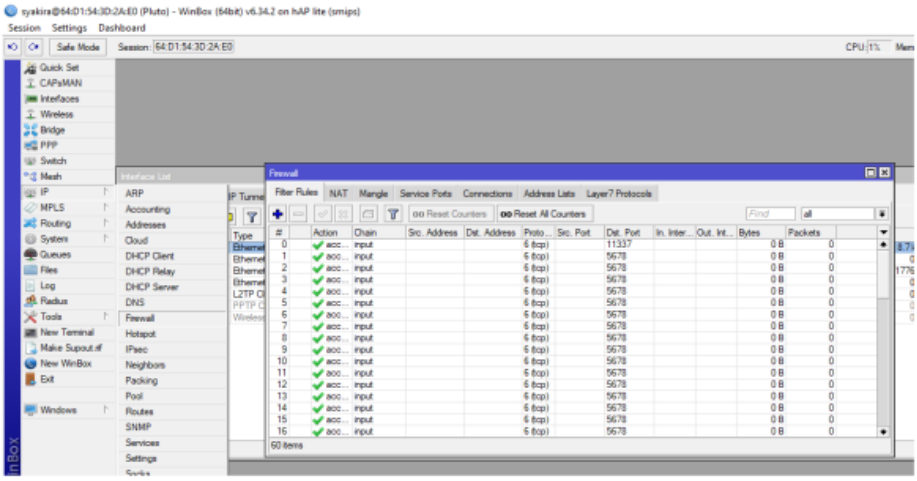
BAB III
FIREWALL

Untuk melindungi router dari akses yang tidak diinginkan dari pihak luar (Internet) dan klien (lokal) maka kita bisa gunakan fungsi firewall. Selain itu, firewall juga digunakan Untuk menyaring akses antar jaringan yang melewati router. Firewall diimplementasikan dalam fungsi filter dan NAT pada mikrotik.

Aturan yang ini disebut aturan penyaringan (filter) firewall, di mana aturan ini diatur dalam rantai (chain) yang ada pada firewall. Ada 3 rantai secara default, yaitu input (ke router), forwarding (dari router), dan output (melalui router) di dalam firewall filtering. Rule yang dibuat akan dibaca terlebih dahulu oleh router dari atas ke bawah pada setiap chain. Kondisi atau persyaratan dalam rantai akan disesuaikan dengan paket, dan jika sesuai, paket akan melewati kondisi atau persyaratan rantai berikutnya/berikutnya. Untuk konfigurasi bisa melalui Menu IP -> Firewall -> Filter Rules.

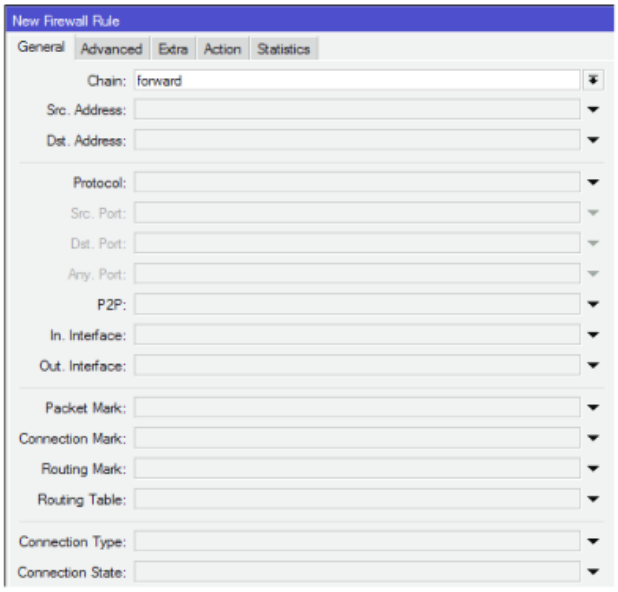


Gambar 3.1. Ilustrasi Aturan Aliran Paket



Gambar 3.2. IP Firewall Filter Rules

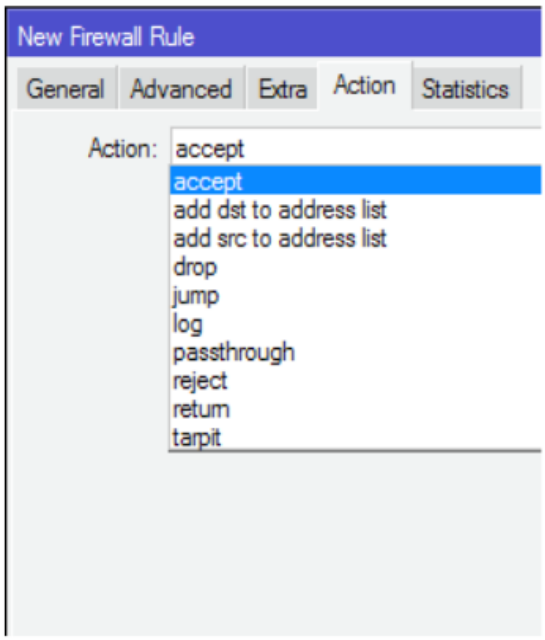
Prinsip IF THEN bisa disimpulkan sebagai "then" yaitu tindakan apa yang akan dilakukan pada paket "jika" memenuhi kondisi yang dibuat dalam atu[illegible]n digunakan di aturan penyaringan firewall. Fungsi ini bisa kita lakukan di Menu IP -> Firewall -> Filter Rules -> General untuk membuat rule IF (kondisi). Lalu kita isi Source IP (IP client), Destination IP (IP Internet), Protocol (TCP/UDP/ICMP, dll.), Source port (biasanya client port), Destination port (destination service port), Interface (masuk atau keluar) traffic) dan paket mask (paket yang dikirim sebelumnya).



Gambar 3.3. Firewall – IF Condition

Untuk konfigurasi *Firewall THEN (action)* bisa kita lakukan di menu *IP->Firewall->Filter Rules->Action*. Jika Paket diterima dan tidak dilanjutkan membaca baris berikutnya maka yang berjalan adalah fungsi Accept. Jika Menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP) maka yang berjalan adalah fungsi Drop. Lalu jika menolak paket dan mengirimkan pesan penolakan ICMP yang berjalan adalah fungsi Reject. Jika "melompati" suatu paket dan menuju ke chain lain yang ditentukan oleh nilai parameter jump target, maka yang berjalan adalah fungsi Jump. Dan jika menolak paket, tetapi tetap menjaga TCP connection yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk), artinya yang berjalan adalah fungsi Tarpit.

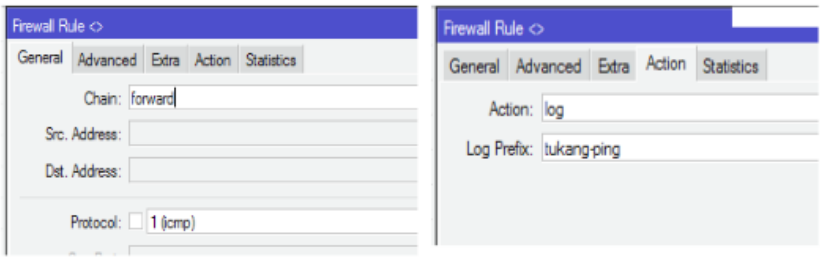
Jika mengabaikan suatu rule dan menuju ke rule selanjutnya, maka yang berjalan adalah fungsi Passthrough. Jika menambahkan informasi paket data ke log, maka yang berjalan adalah fungsi log.



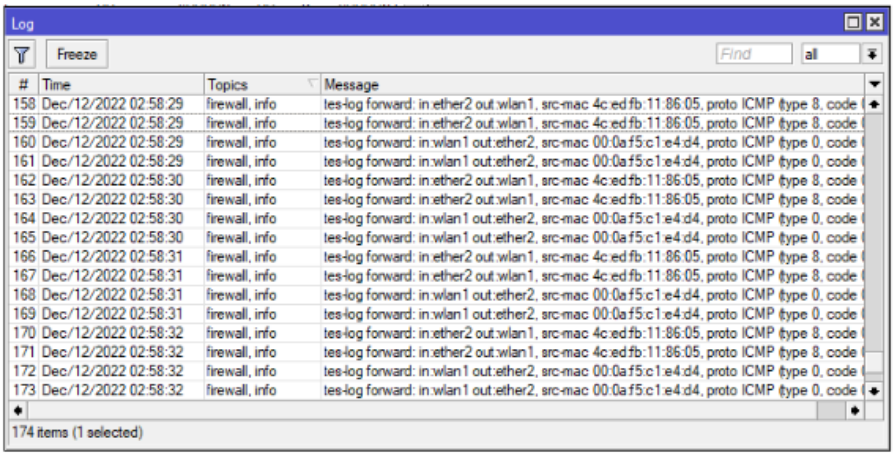
Gambar 3.4. Firewall - Action (Then)

Firewall logging adalah fitur yang merekam (menampilkan dalam log) setiap aktivitas di jaringan yang kita inginkan. Untuk melakukan ini, pada menu IP>Firewall>Filter Rules untuk mencatat semua ICMP ke antarmuka wlan1 kita dapat membuat aturan filter. Untuk menngunakannya, Siapkan

rantai (chain) seperti penerusan atau input menggunakan protokol icmp dan log action. Isi prefix log (isi boleh bebas), sehingga log prefix ini akan muncul di log sebagai deskripsi nama. Setelah itu, kita dapat melakukan ping ke antarmuka IP laptop wlan1 dan kita dapat mengamati log pada router.



Gambar 3.5. Firewall Loging



Gambar 3.6. Log pada Router

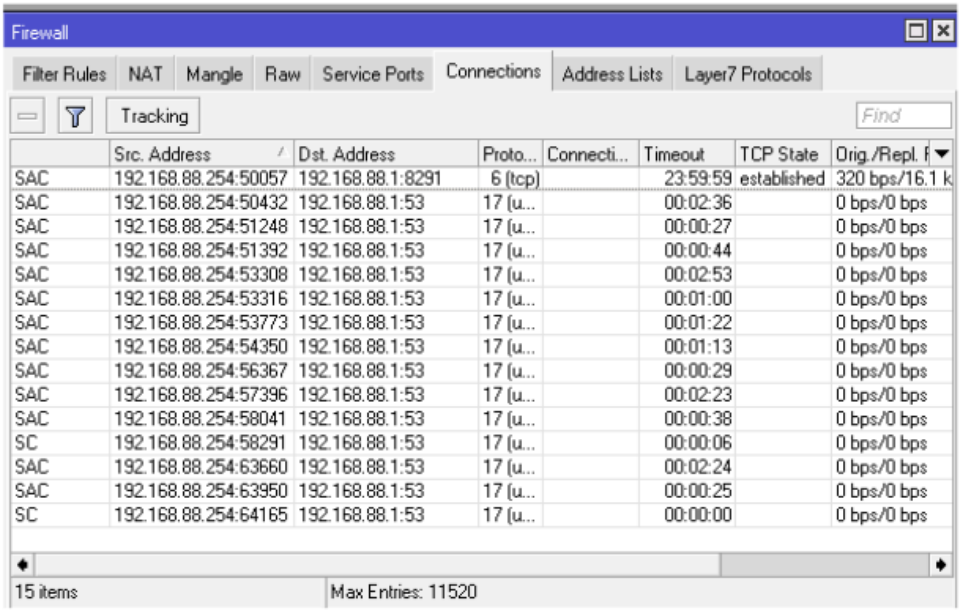
Fitur untuk melihat informasi koneksi seperti IP sumber dan tujuan dan port yang digunakan, status koneksi dan jenis protokol, dan banyak lagi adalah fungsi Tracking Connection. Pelacakan koneksi dapat dilihat di Menu IP > Firewall > Connections. Status koneksi dalam pelacakan koneksi adalah:

- Paket yang dikirim dari bagian dari koneksi yang diketahui disebut ***Established***.
- Paket yang dimulai dari koneksi baru atau milik koneksi yang belum melihat paket di kedua arah disebut dengan ***New***.

- Paket yang dimulai oleh koneksi baru, tetapi terkait dengan koneksi yang ada, seperti transfer data FTP atau pesan kesalahan ICMP disebut ***Related***.
- Paket yang bukan milik koneksi yang diketahui dan tidak ada koneksi baru yang valid disebut dengan ***Invalid***.

Pada baris paling atas umumnya akan dibuat rule pada saat membuat firewall adalah sebagai berikut:

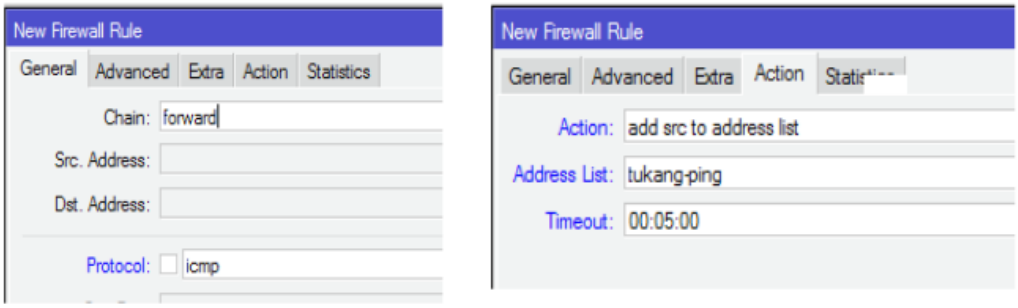
- *Drop* untuk *Connection state invalid*
- *Accept* untuk *Connection state established*
- *Accept* untuk *Connection state related dan new*



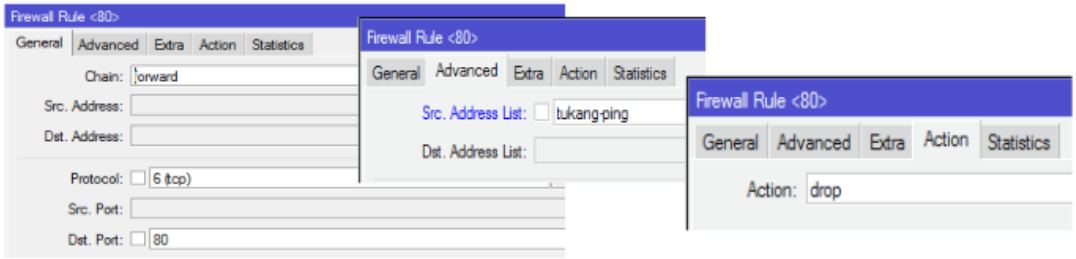
Gambar 3.7. Connection Tracking

Daftar alamat (address list) biasanya digunakan untuk menyaring kelompok alamat IP dengan 1 aturan firewall. Selain itu, tindakan "add to address list" daftar alamat juga dapat berupa daftar hasil IP dari aturan firewall. daftar alamat dapat berupa subnet, range, atau 1 alamat IP host dalam satu baris. Kita dapat membuat aturan firewall yang menyertakan tiap-tiap IP yang di ping ke dalam daftar alamat dan memberi nama pada daftar

alamat. Kemudian kita membuat aturan untuk blok browsing (port 80) sebelumnya dari daftar alamat yang kita buat tadi.

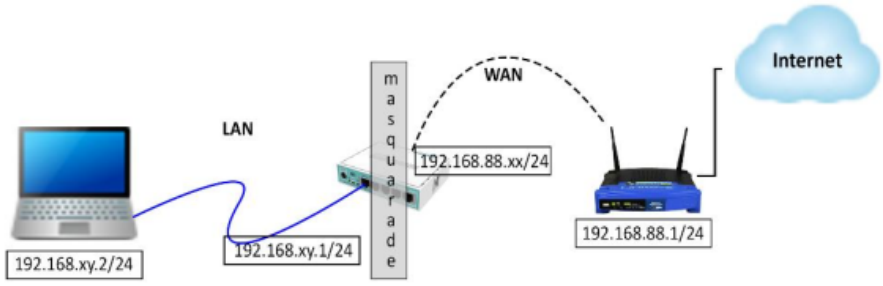


Gambar 3.8. Membuat Rule Firewall – Address List



Gambar 3.9. Address List – Blok Browsing

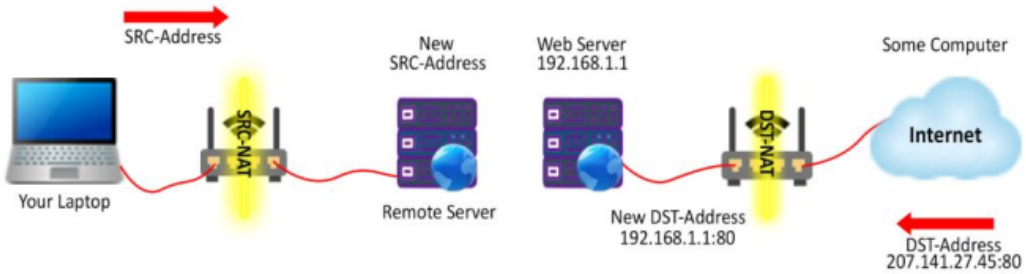
Metode menghubungkan beberapa komputer ke jaringan internet menggunakan satu atau lebih alamat IP disebut dengan NAT (masquerading). Terbatasnya ketersediaan alamat IP publik melatarbelakangi penyebab NAT dipakai hingga saat ini. Selain itu untuk alasan keamanan, kemudahan dan fleksibilitas manajemen jaringan menyebabkan NAT juga dipakai.



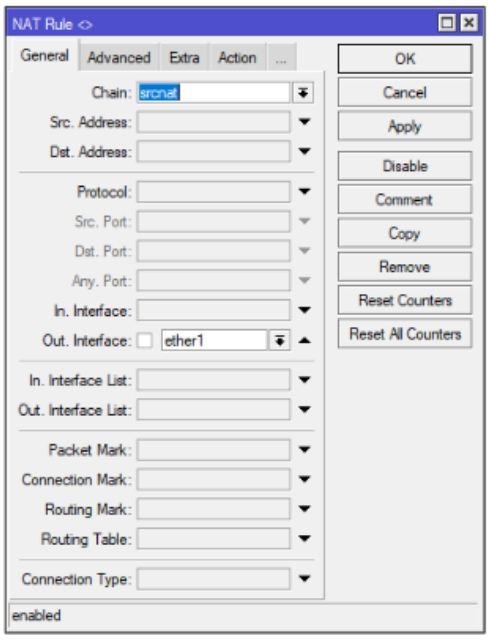
Gambar 3.10. Ilsutrasi NAT Masquerade

Source NAT/srcnat diterapkan pada paket-paket yang berasal dari jaringan di NAT (private/local network) dan NAT/dstnat tujuan diterapkan pada paket-paket yang masuk ke jaringan, keduanya merupakan jenis NAT firewall Mikrotik, biasanya digunakan untuk Access layanan tertentu di jaringan dari luar. Dengan action=masquerade ini, setiap komputer pengguna di jaringan LAN akan diwakili oleh antarmuka (interface) router yang terhubung langsung ke jaringan Internet.

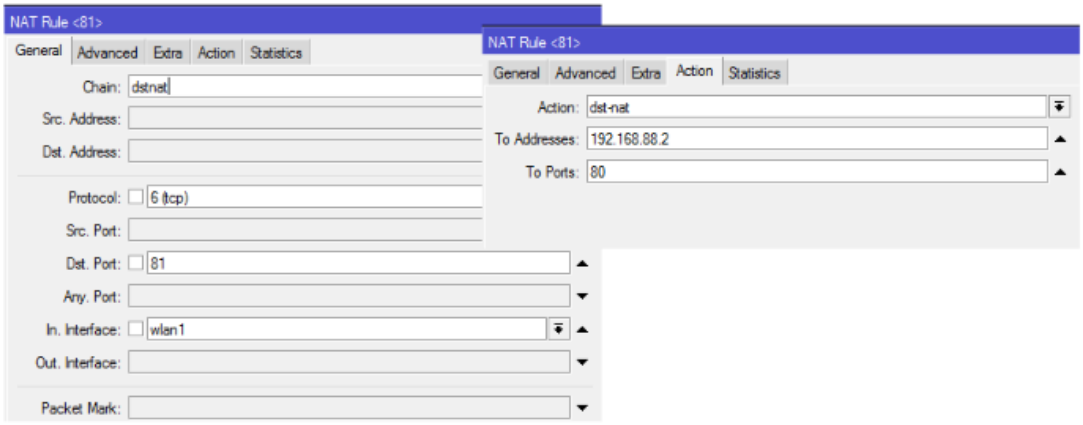
Konfigurasi melalui WinBox dapat dilakukan dengan cara membuka menu IP -> Firewall -> NAT -> General, lalu pilih srcnat pada chain, pilih ether1 untuk output interface, dan selanjutnya pilih Masquerade untuk tab Actions.



Gambar. 3.11. Ilustrasi srcNAT dan dstNAT



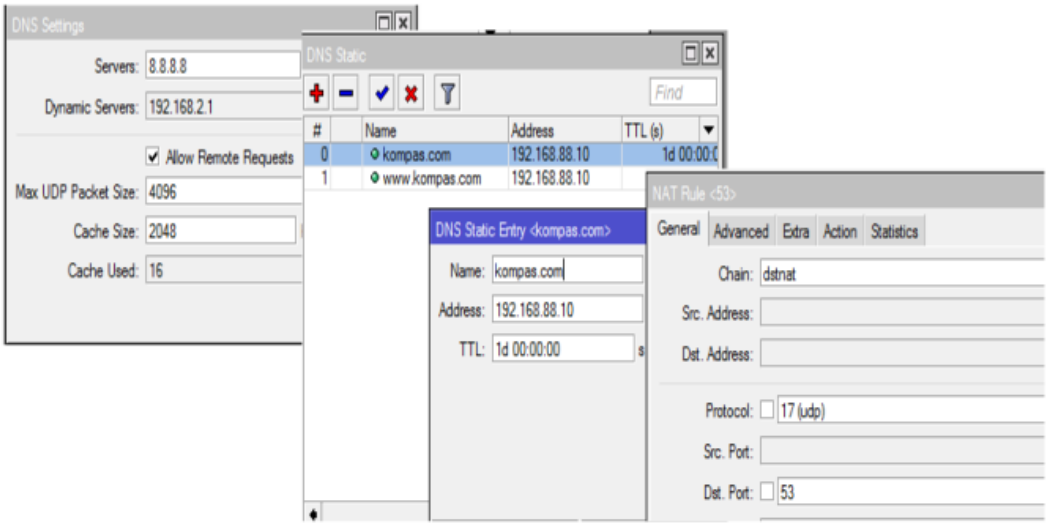
Gambar 3.12. Seting srcNAT



Gambar 3.13. Seting dstNAT

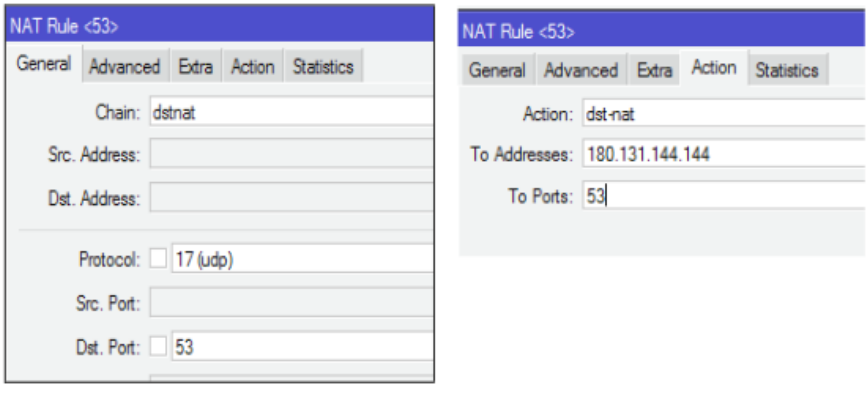
Untuk menerjemahkan nama domain menjadi alamat IP maka kita menggunakan Domain Name System. Daripada alamat IP (203.190.241.43), kita lebih mudah mengingat nama domain seperti detik.com. Dari alamat domain dan alamat IP yang diperoleh dari DNS primer, nantinya DNS memiliki database dan cache. Nantinya cache digunakan Klien yang menggunakan server DNS. Cache akan diperbarui dari server DNS di dalamnya selama periode tertentu.

Metode redirect atau pengalihan satu alamat domain ke alamat domain lain diartikan sebagai static DNS. Pada tabel DNS, kita dapat memanipulasi cache DNS menggunakan entri statis. Dengan masuk ke menu IP > DNS maka IP addressnya adalah 192.168.88.2, kita bisa menambahkan domain misalnya kompas.com, nantinya akan di redirect ke IP address tersebut. 192.168.88.1 jika ingin mengakses website tersebut.



Gambar 3.14. Seting Static DNS

User yang sudah mahir dalam jaringan komputer dapat dengan mudah mengubah pengaturan DNS mereka sendiri, sehingga Transparent DNS dibuat untuk meminimalisir. DNS transparan adalah DNS yang tidak dapat dilihat oleh klien. Agar tidak terlihat, paket harus dikirim langsung ke router (firewall NAT). Jadi DNS tidak ada hubungannya dengan PC dan disetel langsung di router. Fitur ini dapat kita gunakan untuk memblokir akses ke situs-situs terlarang seperti situs judi, situs porno, SARA, dll. Misalnya, kita akan menggunakan bantuan DNS Nawala untuk membantu memblokir situs-situs terlarang tersebut. DNS transparan akan memaksa pengguna untuk mengakses server DNS tertentu. Masuk ke menu IP > Firewall > NAT untuk redirect protokol TCP dan UDP port 53 ke IP Nawala port DNS 180.131.144.144 untuk membuat rule baru.



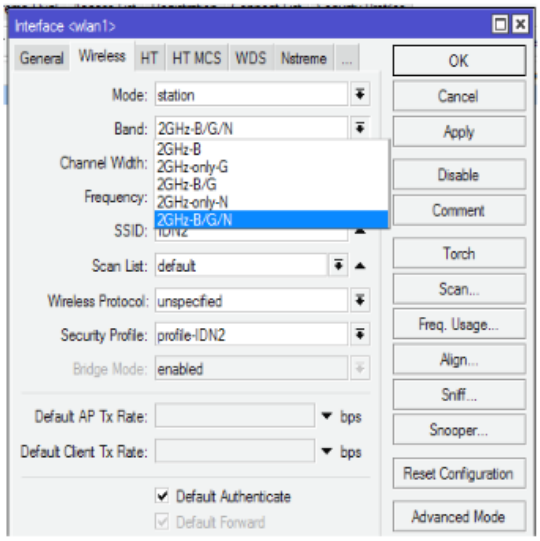
Gambar 3.15. Transparent DNS dengan Nawala

BAB IV
WIRELESS

Wireless dapat diartikan sebagai jaringan yang menghubungkan perangkat telekomunikasi tanpa menggunakan media kabel (nirkabel) sebagai media transmisinya. Perangkat menjalankan fungsi router dan fungsi akses point atau disingkat AP nirkabel pada router nirkabel. Untuk penyediakan akses ke Internet atau jaringan komputer pribadi bisa juga menggunakan router nirkabel. Sederhananya, router bekerja dengan menghubungkan perangkat di jaringan dengan meneruskan paket antar perangkat. Dari satu perangkat ke perangkat lain nantinya data akan dikirim, atau dari satu perangkat ke koneksi internet. Dukungan beberapa modul radio (card wireless) untuk jaringan WLAN atau Wi-Fi (Wireless Fidelity) juga ada di Router OS. Spesifikasi IEEE 802.11 dan menggunakan frekuensi 2.4GHz dan 5GHz ada di modul Wifi. Jenis IEEE 802.11a/b/g/n/ac didukung oleh Router Mikrotik:

- 802.11a – frekuensinya 5GHz dengan kecepatan hingga 54Mbps.
- 802.11b – frekuensinya 2,4GHz dengan kecepatan hingga 11 Mbps.
- 802.11g – frekuensinya 2,4GHz dengan kecepatan hingga 54Mbps.
- 802.11n (Level 4 keatas) – frekuensinya 2,4GHz atau 5GHz dengan kecepatan hingga 300Mbps
- 802.11ac (Level 4 keatas) – frekuensinya 5GHz dengan kecepatan hingga 1Gbps

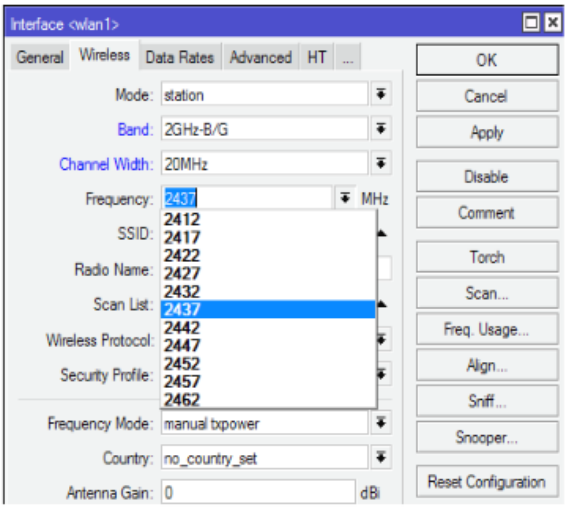
Di sisi nirkabel, router memiliki teknologi pita nirkabel (band), yang merupakan mode kerja frekuensi perangkat nirkabel. Keduanya harus bekerja pada pita frekuensi yang sama jika ingin terhubung antar dua perangkat. Pita frekuensi dalam daftar tergantung pada jenis card wireless. Untuk memilihnya bisa kita lihat di menu Wireless > Interface > Wireless.



Gambar 4.1 Wireless Band di Mikrotik

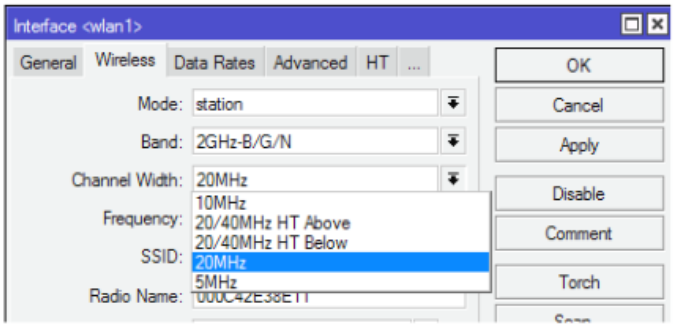
Saluran (frequency) dapat didefinisikan sebagai pembagian frekuensi dalam pita frekuensi tempat akses poin kita beroperasi. Nilai channel saluran tergantung pada pita frekuensi yang dipilih, kemampuan card wireless router, dan peraturan frekuensi nasional. Channel saluran untuk setiap band berkisar dari 2,4Ghz = 2412 hingga 2499MHz dan 5GHz = 4920 hingga 6100MHz. Aturan atau regulasi tertentu mengenai frekuensi nirkabel internet dimiliki dan diatur oleh setiap negara. Berdasarkan KEPMENHUB No. 2/2005 dan berkat kerja keras Pegiat Internet sejak 2001, Indonesia telah disetujui untuk menggunakan frekuensi 2.4GHz. Tuning frekuensi di mikrotik didefinisikan di bagian "Country Regulation" Nirkabel. Jika Kita ingin mengaktifkan semua frekuensi kartu nirkabel, gunakan opsi "superchannel".

Pada mode frekuensi terdapat tiga pilihan yaitu daya pancar manual (manual tx power), artinya daya pancar diatur secara manual (tidak disesuaikan untuk beberapa negara). Mengatur frekuensi channel dengan frekuensi yang diperbolehkan di suatu negara ada di bagian domain regulasi. Membuka semua frekuensi yang dapat didukung oleh card wireless ada di bagian superchannel. Di Antenna Gain, defaultnya adalah 0, yang berarti tidak akan secara otomatis melebihi EIRP dari peraturan negara yang dipilih.



Gambar 4.2. Frequency Channel

Rentang frekuensi bawah dan atas dalam satu channel saluran didefinisikan sebagai Channel Width. Mengatur lebar saluran channel width yang digunakan bisa menggunakan router Mikrotik. Default dari channel width adalah 22MHz (ditulis sebagai 20MHz), Untuk meminimalkan frekuensi lebar channel width dapat dikurangi (5MHz), atau untuk mendapatkan throughput besar bisa ditingkatkan (40MHz).



Gambar 4.3. Channel Width

Dalam satu atau lebih station, diterapkan Konsep konektivitas nirkabel adalah bahwa koneksi akan terjadi antara titik akses poin (AP), koneksi juga akan terjadi antar WDS-Slave, atau jika ada kesamaan antara SSID dan Band, Station secara otomatis akan mengikuti saluran di AP. Station hanya dapat

memindai AP yang memiliki daftar saluran yang ditetapkan di station. Interface dari nirkabel adalah sebagai berikut:

1. Mode akses poin (AP)

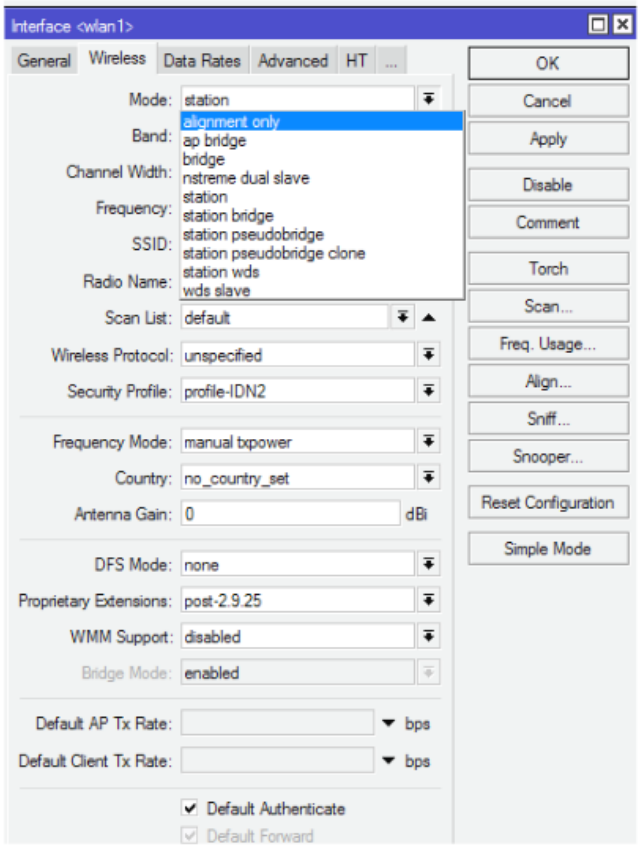
- AP-bridge, pada mode ini wireless dapat digunakan sebagai titik akses.
- Bridge, mode ini mirip dengan AP-bridge, tetapi hanya satu klien yang dapat dihubungkan, mode point-to-point sering digunakan di metode ini.

2. Mode Station

- Station, mode ini memindai dan menghubungkan ke AP jika frekuensi dan SSID sama,tidak dapat *bridge* dengan mode ini.
- Station-bridge, mode ini mirip dengan station di atas, pada MikroTik mode ini sangat eksklusif. Mode untuk bridge L2, kecuali wds.
- Station-wds, mode ini mirip dengan Station juga, tetapi membuat koneksi WDS ke AP yang menjalankan WDS.
- station-pseudobridge, mode ini mirip dengan station juga, namun dengan penambahan terjemahan alamat MAC untuk bridge
- station-pseudobridge-clone – mode ini mirip dengan station-pseudobridge, kita bisa gunakan alamat station-bridge-clone-mac pada AP untuk terhubung..

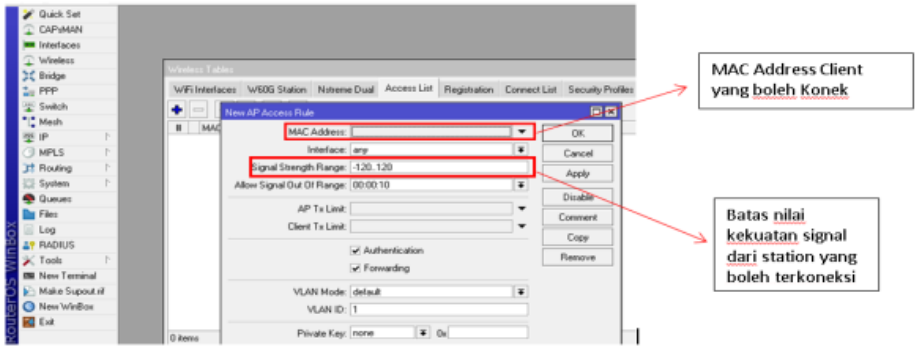
3. Mode Spesial

- Alignment only, pada mode ini pemosisian antena jarak jauh bisa menggunakan mode transmisi.
- nstreme-dual-slave, pada mode ini digunakan untuk sistem nstreme-dual bisa dengan mode ini.
- WDS-slave, mode ini sama seperti ap-bridge dengan cara memindai ke titik AP dengan SSID yang sama dan terhubung dengan WDS. Jika tautan koneksi putus, mode ini tetap akan melanjutkan pemindaian koneksi.

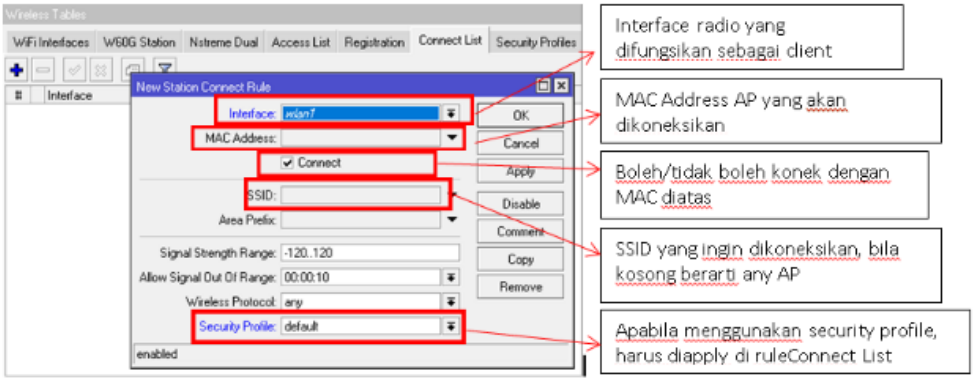


Gambar 4.4. Mode Interface Wireless

Alat akses poin (AP) hanya dapat dihubungkan oleh station yang terdaftar dengan membatasi akses melalui penyaringan MAC wireless pada AP wireless. Pada SSID AP yang sama, station dapat dikunci untuk bisa terhubung ke AP terdaftar. Setiap station yang terdaftar pada titik akses poin, router dapat menyaring station yang dapat dihubungkan. Kita dapat melakukan konfigurasinya di menu Wireless > Access List, jika otentikasi default tidak dicentang pada menu interface (wlan1), maka nantinya daftar akses station menjadi berfungsi.

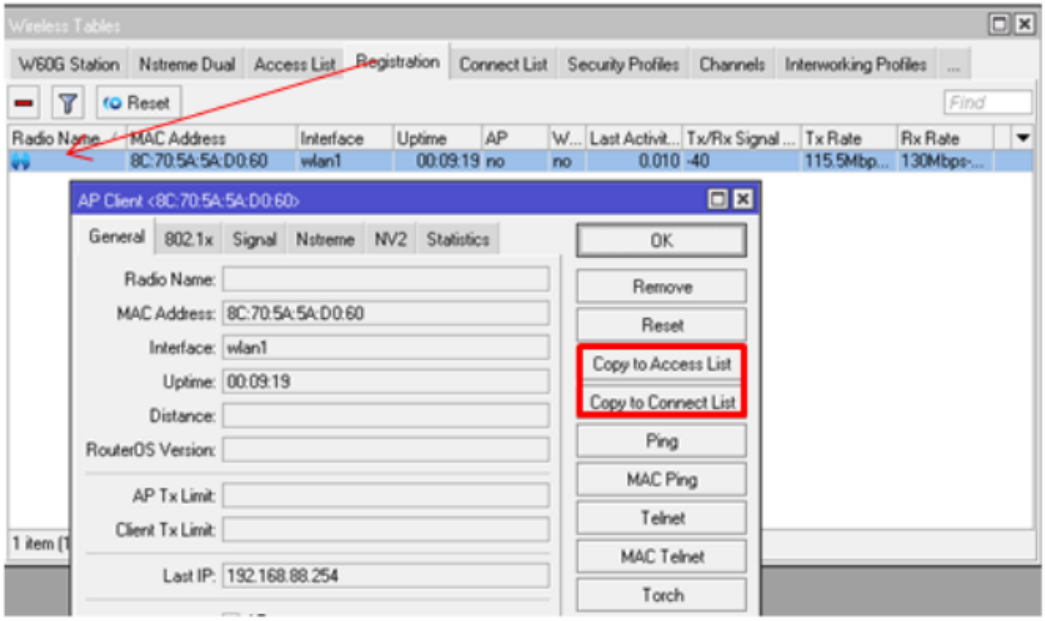


Di menu station wireless, daftar koneksi membatasi titik akses (AP) untuk memilih station mana yang dapat atau tidak dapat terhubung. Kita bisa mengaturnya di daftar Wireless > Connections.



Gambar 4.6. Connect List

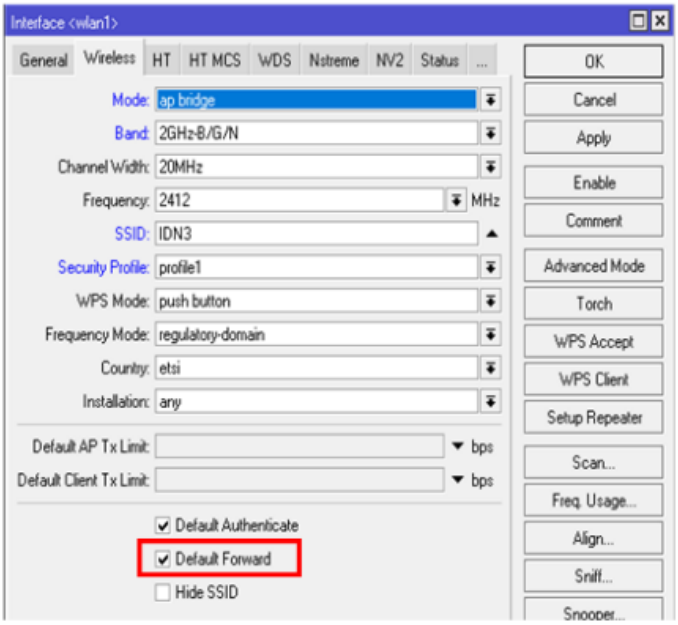
Di menu Regist list berisi data tentang AP atau klien yang saat ini terhubung. Kita bisa menggunakan menu Copy to Access/Connection List untuk memudahkan kita memfilter Access List dan Connection List. Kita dapat mengkonfigurasi menu ini di Wireless > Registration.



Gambar 4.7. Registration List

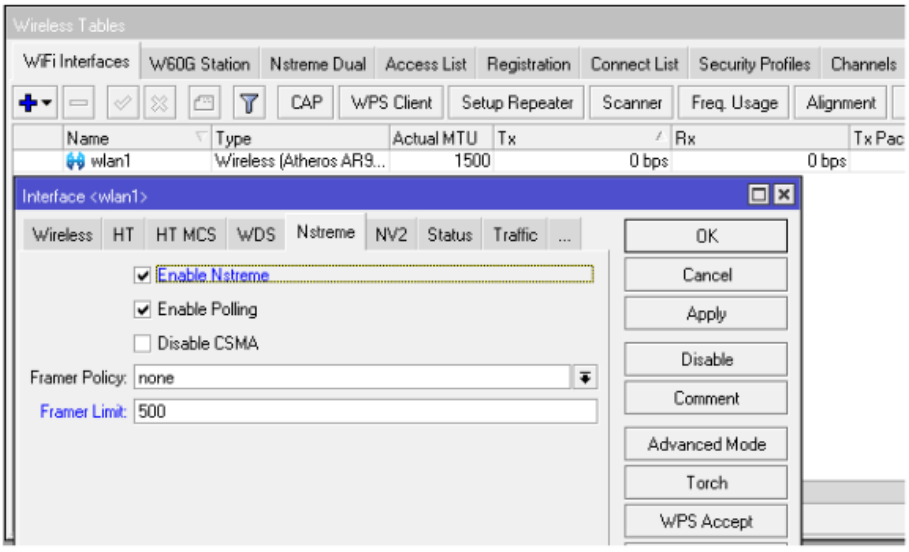
Agar membuat koneksi point-to-point kita tidak mudah tertukar dengan koneksi lain, kita bisa menggunakan fitur MAC Filter pada Router Mikrotik. Caranya adalah dengan memasukkan data alamat MAC wireless partner ke dalam daftar, masukkan ke dalam Connect-List jika station, dan masukkan ke Access-List jika statusnya sebagai AP. Default authentication harus di *uncheck* agar tidak semua client bisa melakukan authenticate secara otomatis untuk wireless setup pada AP. Klien tidak akan dapat terhubung jika kita mencoba untuk terhubung ke AP yang bukan pasangannya.

Fitur drop antar klien digunakan untuk mengizinkan atau melarang komunikasi antara klien/workstation yang terhubung ke titik akses (AP) yang sama. Untuk konfigurasi fungsi ini, kita bisa mengaturnya di menu wireless > interface. Untuk tujuan keamanan klien hotspot, penerusan (forward) default biasanya "dinonaktifkan", bagian ini hanya dapat dikonfigurasi di sisi titik akses (AP).

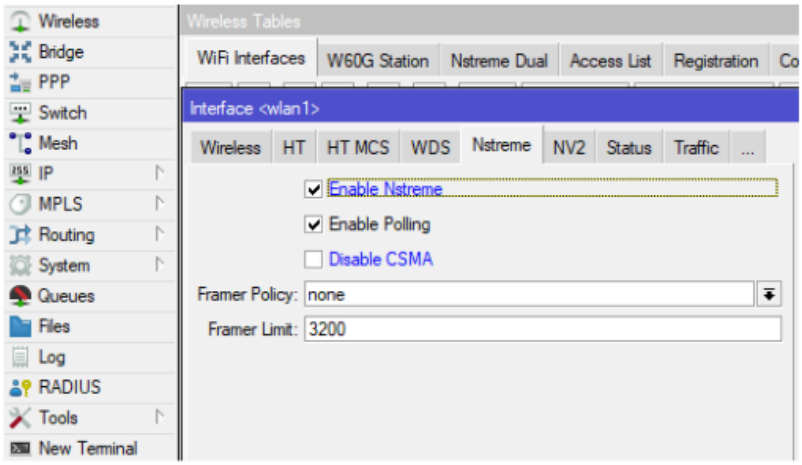


Gambar 4.8. Drop Koneksi Antar Client

Fitur Nstreme merupakan salah satu keunggulan yang dipunyai oleh router Mikrotik. Tujuannya untuk meningkatkan kemampuan wireless untuk melakukan koneksi terutama yang jaraknya jauh. Fitur ini harus diaktifkan pada AP dan client, dan konfigurasi hanya pada sisi AP (Access Point).



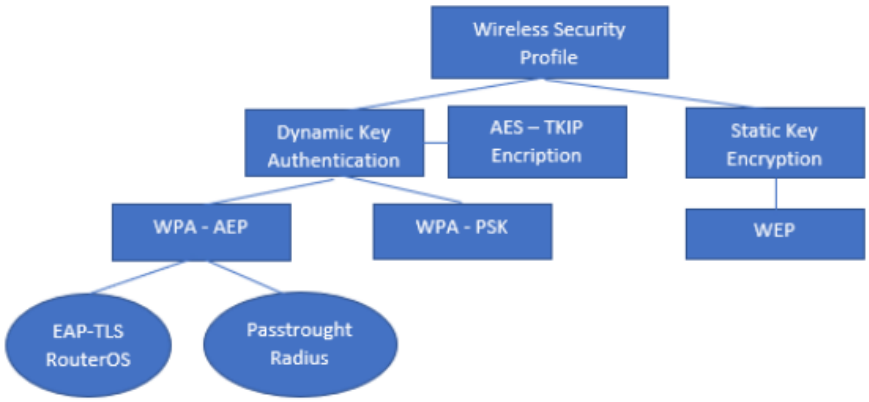
Gambar 4.9. Seting Wireless Nstreme di Access Point



Gambar 4.10. Seting Wireless Nstreme di Station

Untuk mengamankan koneksi tanpa kabel, mikrotik memiliki banyak cara untuk melakukan filter MAC, karena data yang lewat dapat dianalisis. Ada beberapa metode keamanan yang digunakan jaringan tanpa kabel yang umum digunakan, yaitu:

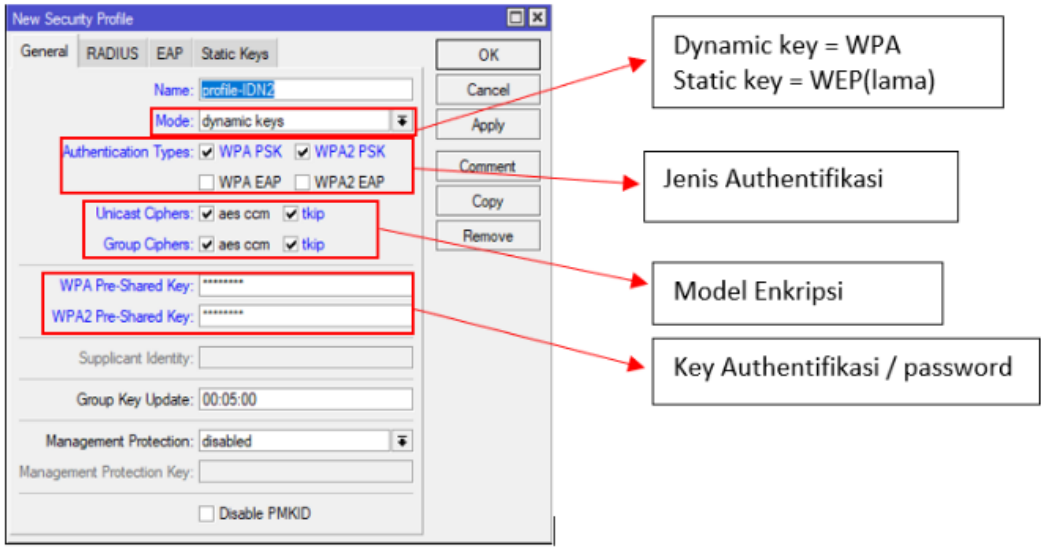
- Metode Authentication (yaitu WPA-PSK, WPA-AEP)
- Metode Enkripsi (yaitu AES, TKIP, WEP)
- Metode Tunnel (tunel)



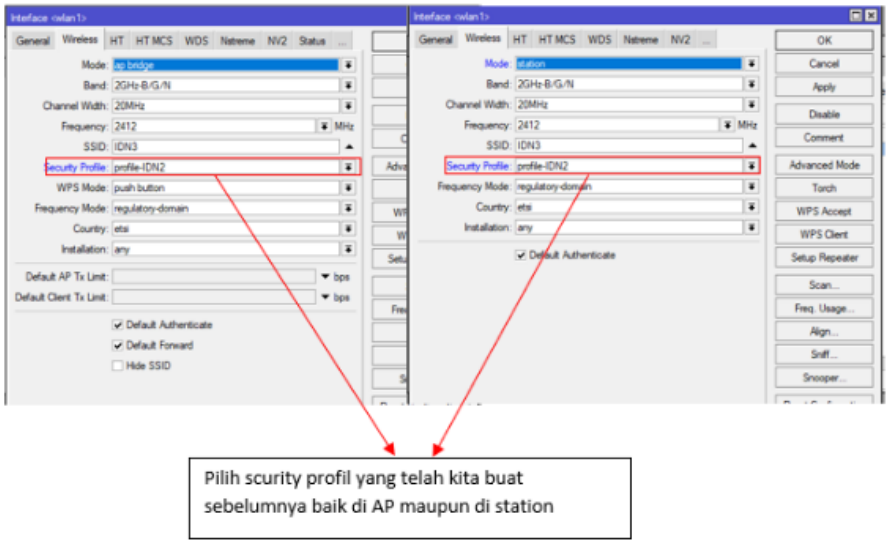
Gambar 4.11. Metode Wireless Security Profile

Menu *Wireless* > *Security Profile* bisa digunakan untuk melakukan enskripsi pada jaringan wireless mode WPA. Diberi nama tertentu agar diimplementasikan dalam interface jaringan wireless pada bagian Security Profile ini. Pada menu *Wireless* > *Interface* > *Wireless* digunakan untuk setingan pada Security Profile tadi di implementasikan pada interface wireless.

Untuk melakukan enkripsi pada jaringan wireless mode WPA, kita bisa melakukannya di Wireless > Security Profile. Bagian profil keamanan diberi nama khusus untuk diterapkan di interface tampilan jaringan nirkabel. Kemudian terapkan pengaturan di profil keamanan pada interface nirkabel di Menu wireless > interface > wireless.

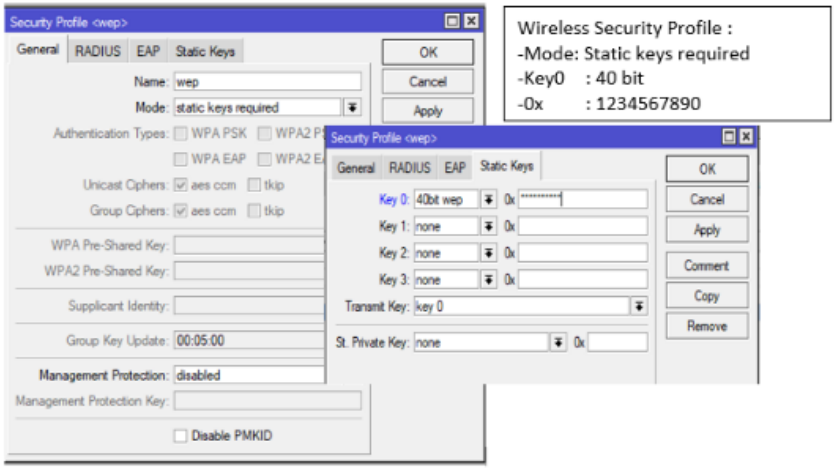


Gambar 4.12. Seting Security Profil WPA



Gambar 4.13. Implementasi Security Profile WPA

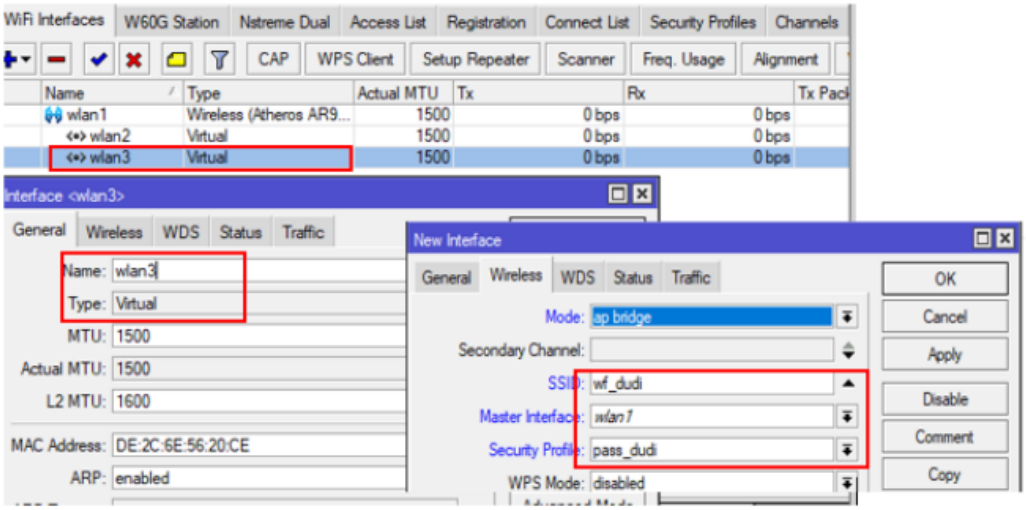
Metode WEP (Wired Equivalent Privacy) merupakan metode yang sederhana dan pertama kali muncul serta digunakan untuk profil keamanan,. Metode ini tidak memiliki metode otentikasi dan oleh karena itu kurang disarankan penggunaannya karena dapat dengan mudah diretas.



Gambar 4.13. Implementasi Security Profile WEP

Kita dapat menggunakan VAP (Virtual Acces Poin) yang ada di Mikrotik untuk membuat beberapa SSID dalam satu interface wireless (Microtik internal access point) dengan layanan yang berbeda atau sama.

Nantinya akan menjadi “child” dari wlan (interface asli) dari AP virtual ini. Pada VAP kita bisa memiliki beberapa interface (hingga 128). Pada AP virtual dengan SSID, profil keamanan (security profile), dan list akses yang berbeda dapat kita atur, dengan tetap sama dengan wlan induk pada frekuensi dan band. Virtual AP ini persis sama dengan AP karena dapat terhubung ke station/klien, dapat bertindak sebagai server DHCP, dan dapat bertindak sebagai server hotspot. Untuk pengaturan, Kita dapat pergi ke Wireless Menu > Interface > Add dan pilih Tipe untuk VirtualAP. Kemudian atur pada tampilan baru yang kita buat (misalnya wlan2, wlan3)



Gambar 4.14. Virtual Access Point

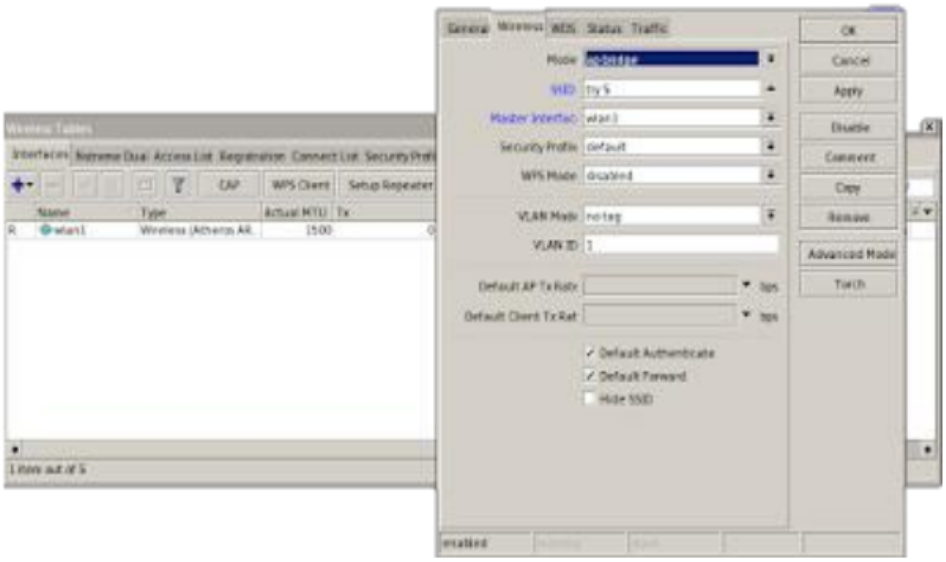
BAB V
BRIDGE

Bridge bisa diartikan sebgaia upaya untuk menggabungkan 2 atau lebih interface tipe Ethernet seolah-olah berada pada segmen jaringan yang sama adalah definisi dari bridge. Mode ini juga bekerja pada jaringan wireless. Mode bridging ini beroperasi pada lapisan OSI kedua (link layer). Antarmuka (interface) yang dijembatani adalah interface yang virtual. Membuat bridge baru dan kemudian menambahkan antarmuka fisik ke port bridge adalah tahapan awal pembuatan bridge ini. Bridge akan dianggap hanya sebagai interface loopback jika kita membuat atau menambahkan interfce bridge, tetapi tidak menambahkan interface fisik ke port. Mode bridge memiliki beberapa kelemahan, antara lain:

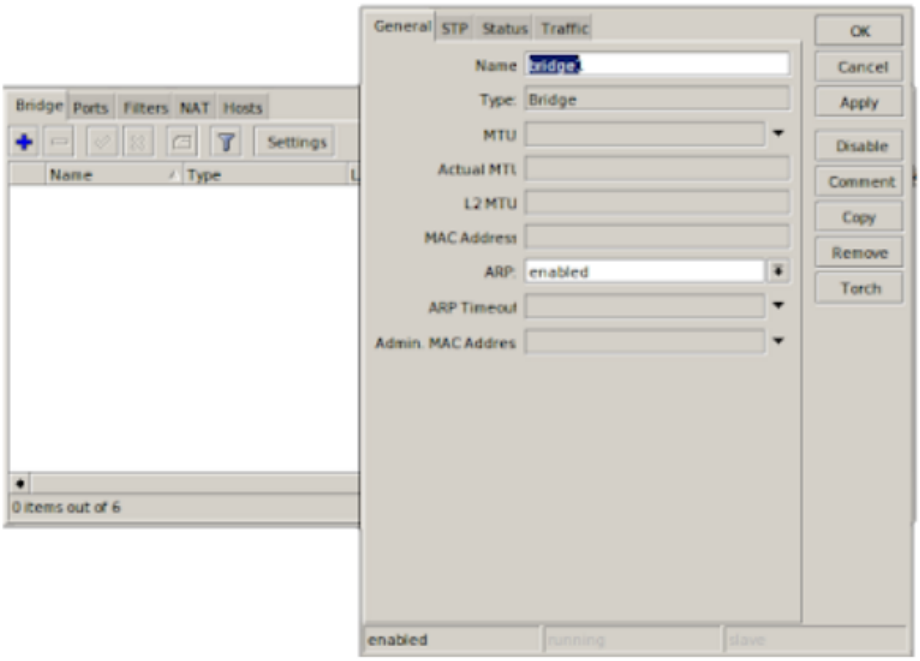
- Kesulitan mengatur lalu lintas (traffict) dari broadcast seperti virus komputer.
- Semua segmen pada bridge yang sama akan terpengaruh dan bermasalah jika ada suatu segmen yang juga bermasalah.
- beban lalu lintas meningkat karena akumulasinya

A. Bridging Wireless

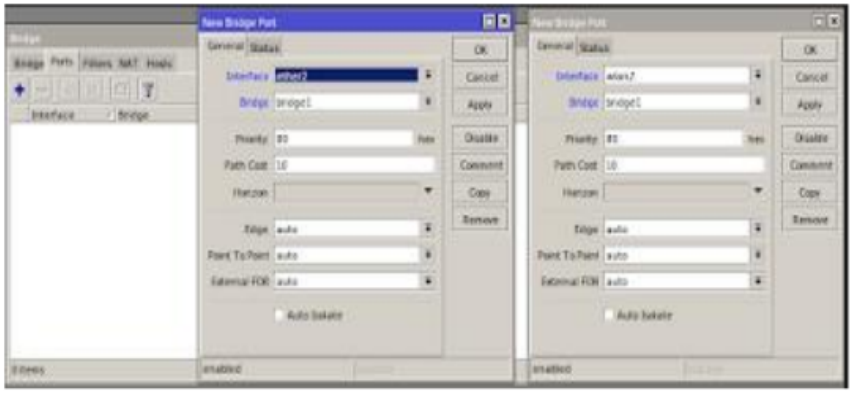
MikroTik memungkinkan kita menggunakan fitur untuk menjembatani station sejak versi 5 Mikrotik diluncurkan, fitur ini disebut Station Bridge. Station bridge ini hanya bekerja pada koneksi antar MikroTik, minimal kita harus menggunakan Mikrotik versi kelima. Kita dapat melakukan konfgurasinya melalui Menu Wireless > Interface > Add > Wireless untuk membuat bridge dari sisi AP. Kita juga bisa membuat SSID dan password pada bridge dan mengatur nama bridge sesuai kebutuhan.



Gambar 5.1. Seting AP Bridge

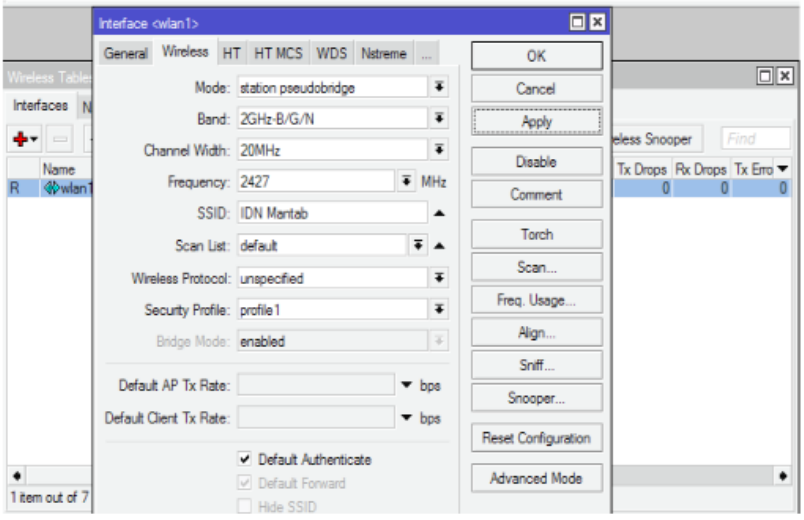


Gambar 5.2. Mengisi Nama Bridge

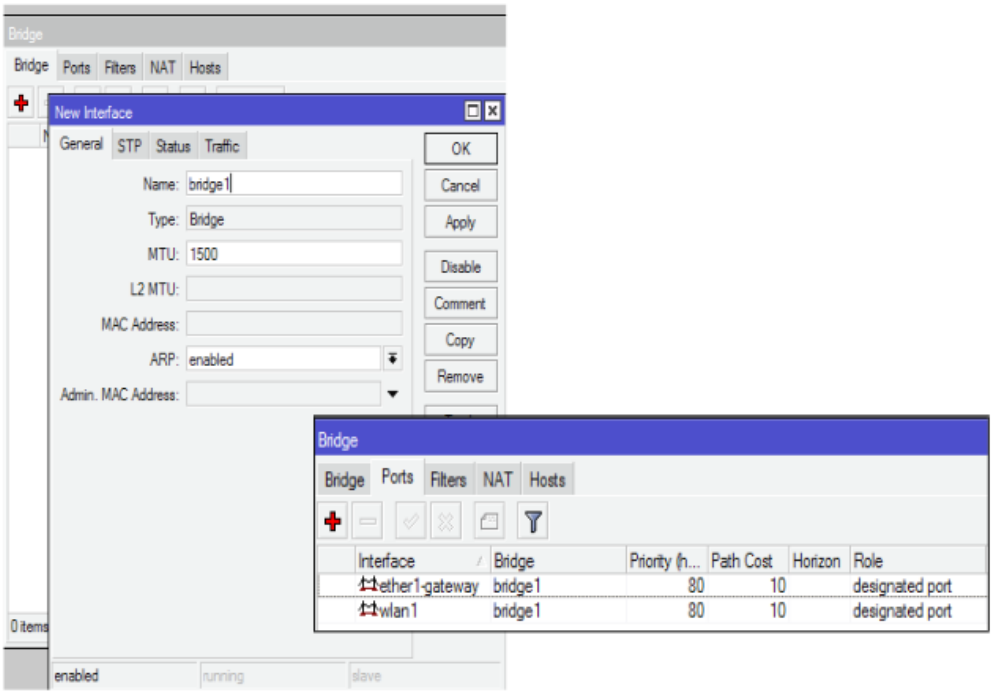


Gambar 5.3. Bridge Interface (eth) yang terhubung dengan Client – Wlan AP

Selain mode station bridge standar, ada juga mode station - psudobridge (bridge nirkabel sederhana), yang merupakan pengembangan dari mode station standar, semuanya menggunakan koneksi nirkabel sebagai penerima/klien, perbedaannya adalah station-pseudobridge mendukung pembuatan jaringan yang dibridge, saat menggunakan mode ini, akan menyebabkan bridging yang tidak sepenuhnya karena alamat MAC berada di bawah perangkat nirkabel (end user PC) tidak akan terbaca di bagian titik akses (AP). Kita dapat mengkonfigurasinya pada menu Wireless > Interface > Add > Wireless. Setelah itu buat juga interface bridge dan tambahkan interface eth1 dan wlan1 ke port. Kemudian atur IP DHCP (Dynamic IP Address) pada klien PC/Laptop.



Gambar 5.4. Seting Station Pseudobridge



Gambar 5.5. Membuat dan menambahkan interface eth dan wlan pada port

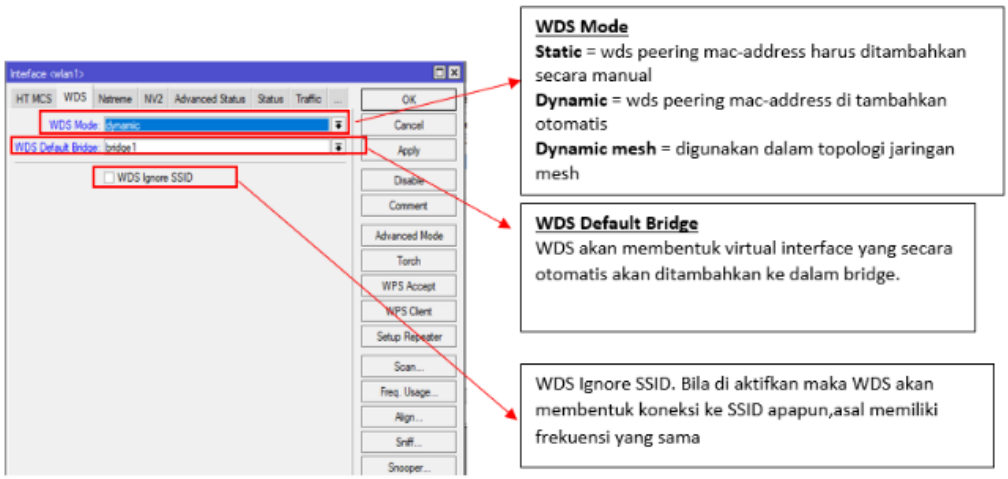
B. Wireless Distribution System (WDS)

Istilah Wireless repeater sering digunakan sebagai pengganti istilah WDS, yaitu sistem yang digunakan untuk mengembangkan jaringan nirkabel tanpa menggunakan media transmisi kabel jaringan, tetapi menggunakan perangkat yang disebut perangkat repeater atau access point (AP) . Untuk membuat jaringan nirkabel yang berskala besar, kita bisa membuatnya dengan menghubungkan beberapa titik AP. Biasanya system ini digunakan untuk membangun jaringan besar yang tidak dapat menggunakan kabel atau mahal jika menggunakan banyak kabel, memiliki area terbatas, atau secara fisik tidak mampu menarik kabel maka umumnya menggunakan mode WDS ini. Di Mikrotik ada beberapa jenis WDS :

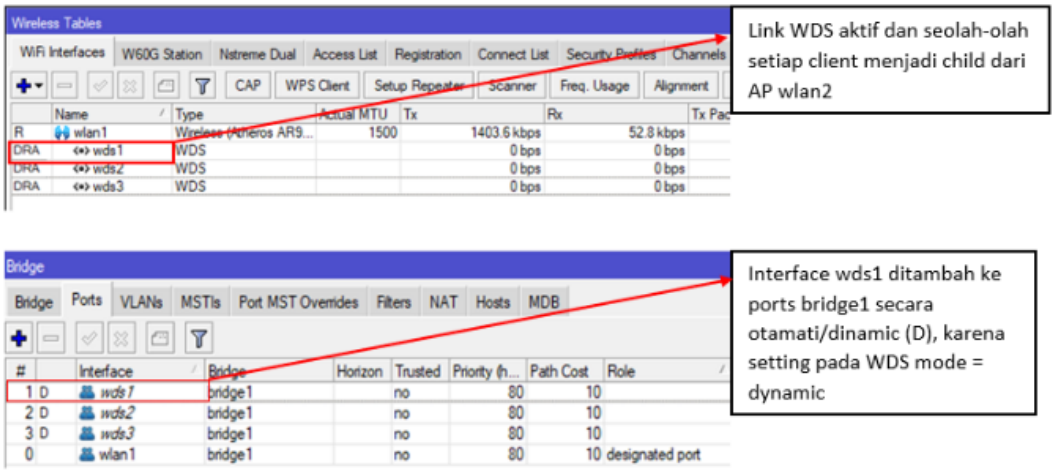
- WDS Statis
- Dinamis WDS
- Mesh WDS

Cara melakukan konfigurasi pengaturannya dengan membuka WDS melalui menu Wireless > klik Wlan (misalnya Wlan1) > WDS. WDS peering

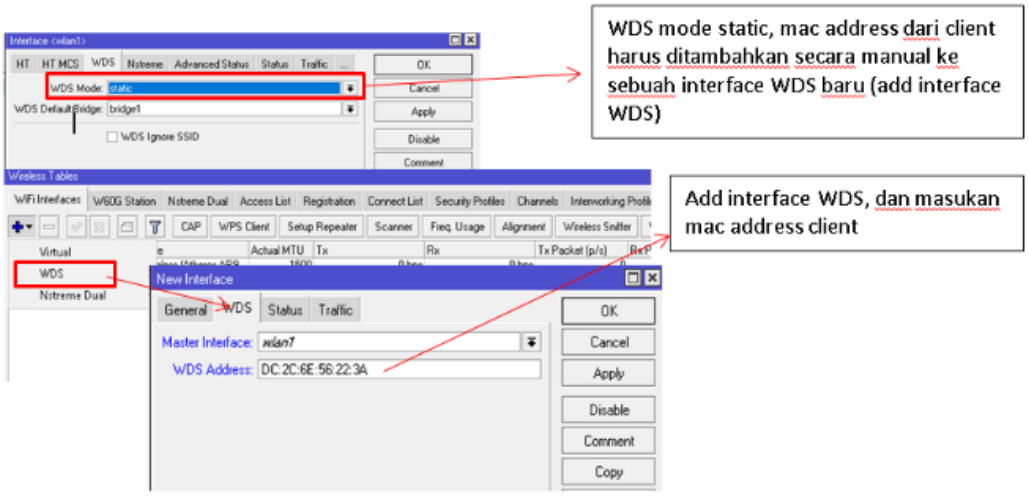
mac-address yang harus ditambahkan secara manual disebut dengan WDS static mode, lalu ada yang namanya WDS peering mac-address jika ditambahkan secara otomatis kemudian ada yang disebut dengan dynamic mesh yang digunakan untuk topologi mesh disebut WDS Dynamic.



Gambar 5.6. Konfigurasi WDS Dynamic



Gambar 5.7. Hasil Konfigurasi WDS Dynamic



Gambar 5.8. Konfigurasi WDS Static

BAB VI
ROUTING

Proses penentuan jalur terbaik ke jaringan tujuan, sebagai proses perpindahan sebuah paket dari host pengirim (source) ke host tujuan (destination), dan dilakukan pada jaringan yang berbeda adalah pengertian dari Routing. Proses routing terjadi pada lapisan (layer) ketiga yaitu lapisan jaringan yang berhubungan dengan pengalamatan IP di layer OSI.

Kita membutuhkan perangkat perantara yang disebut dengan router untuk mengimplementasikan teknik ini. Perangkat jaringan dengan beberapa antarmuka interface jaringan yang dapat menentukan jalur terbaik bagi paket untuk mencapai jaringan tujuan adalah fungsi dari Router itu sendiri. Pemindahkan paket yang masuk pada interface satu ke yang lainnya (penerusan paket) dilakukan oleh Router. Beberapa jaringan yang berbeda bisa terhubung dengan Router. Saat ini, Router board yang dilengkapi dengan MikroTik Router OS sebagai sistem operasinya adalah sebuah perangkat router yang banyak digunakan. Jenis-jenis routing adalah jenis statis dan jenis dinamis.

A. Jenis Routing

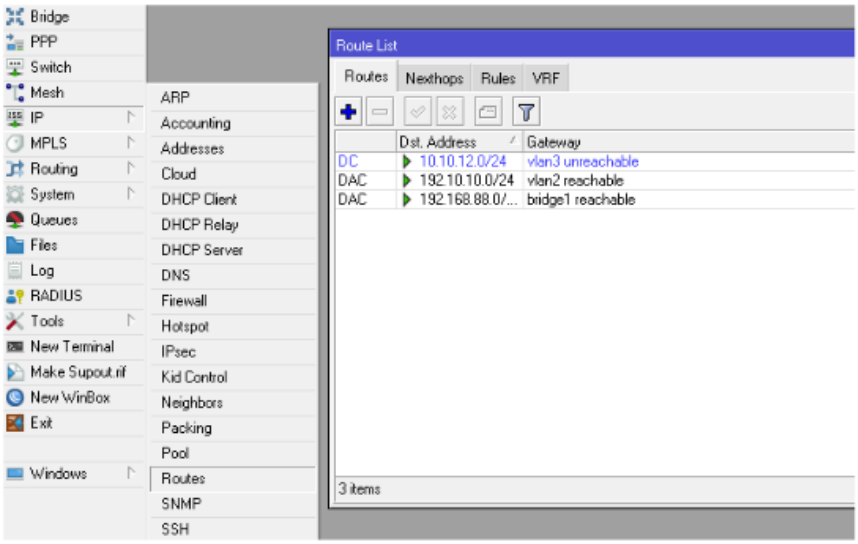
Proses pengaturan router jaringan menggunakan tabel routing yang dikonfigurasikan dengan cara manual oleh admin jaringan disebut dengan Routing Statis. Tugasnya adalah akan mengisi setiap entri dalam forwarding table di setiap router dimana router tersebut terhubung pada jaringan, prinsipnya adalah “mau kemana?” dan “lewat mana?”. Sementara, sebuah router yang memiliki dan membuat tabel routing secara otomatis dengan menggunakan lalu lintas traffic jaringan dan juga saling berhubungan dengan router lainnya disebut Routing Dynamic.

Suatu perangkat di dalam komputer yang fungsinya untuk mengkoneksi sebuah jaringan komputer terhadap satu jaringan komputer lain menggunakan protokol informasi yang tidak sama disebut dengan Gateway. hardware yang berfungsi untuk menghubungkan antar jaringan yang beda disebut dengan router. Meski hampir menyerupai router, router tidaklah sama

dengan gateway. Perangkat yang memancarkan sekaligus menangkap sinyal internet atau membuat sebuah jaringan dapat melakukan akses internet adalah fungsi dari perangkat Router. Sementara pengertian gateway ini, lebih kepada koneksi antar perangkat komputer yang berada di dalam sebuah internet.

Nantinya, istilah S, DAS, AS, ataupun DAC Saat melakukan setting gateway atau routing di Mikrotik mungkin akan kita temui dan disebut dengan istilah flag. Flag-flag tersebut dijelaskan di laman resmi Mikrotik sebagai berikut :

- S diartikan sebagai Route Static
- D diartikan sebagai Dynamic
- A diartikan sebagai Active
- C diartikan sebagai Connect

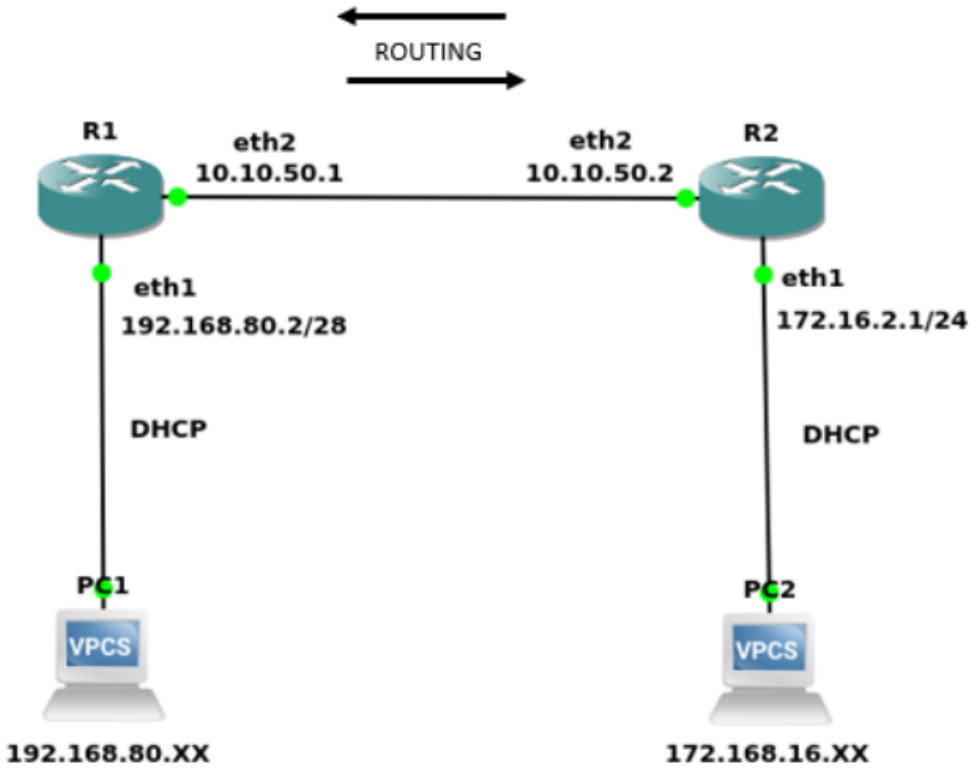


Gambar 6.1. Route Flag

Kita bisa memahami bahwa DAS adalah Dynamic Active Static, yaitu suatu routing bersifat static yang dibuat secara dynamic atau otomatis, lalu DAC adalah Dynamic Active Connect yaitu konfigurasi terhubung yang dibuat secara otomatis dan AS adalah Active Static, yaitu konfigurasi routing yang kita definisikan sendiri dari penjelasan di atas.

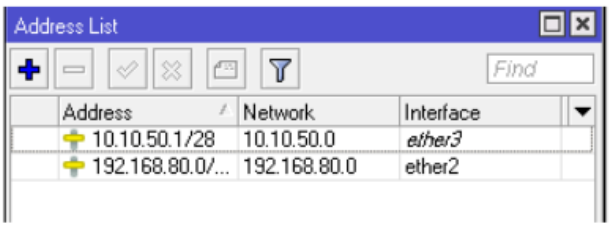
B. Implementasi Routing

Kita akan mencoba membuat koneksi routing statis sederhana sebagai contoh dengan topologi berikut:



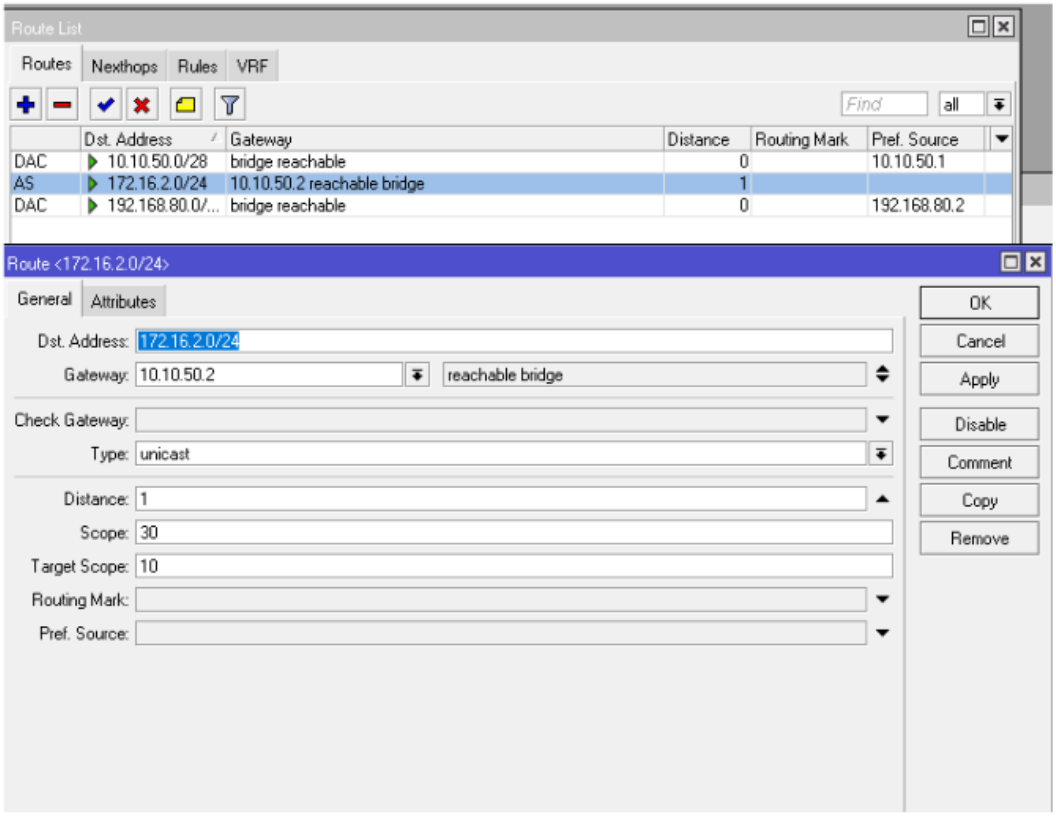
Gambar 6.2. Simulasi Statik Routing Sederhana

Untuk mengaturnya, kita bisa masuk ke *IP > address* lalu kita atur ip-nya router 1 eth3 misalnya ip address 10.10.50.1/28 dan eth2 ip address 192.168.80.2/28 di Winbox.



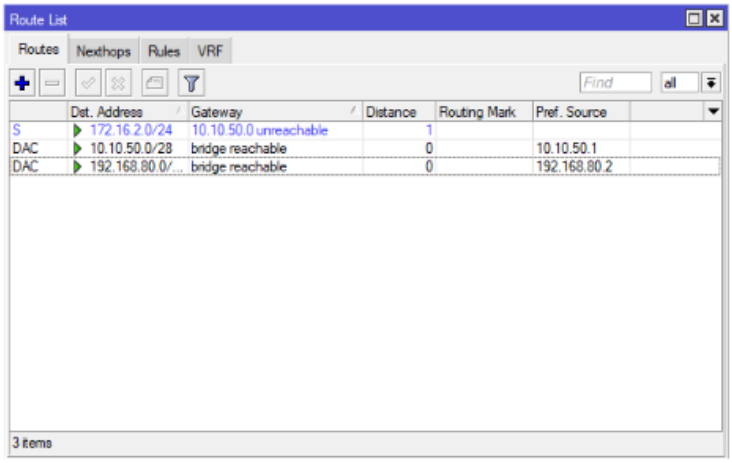
Gambar 6.3. Menambahkan Ip Address Router 1

7 Masuk ke *IP > route > klik add*(+), selanjutnya Dst.Address isikan 172.16.2.0/24 (ip network client yang ada pada router2) dan selanjutnya pada gateway isikan 10.10.50.2 (ip yang terhubung dari router2 ke router1), lalu silahkan klik apply > ok di Winbox.

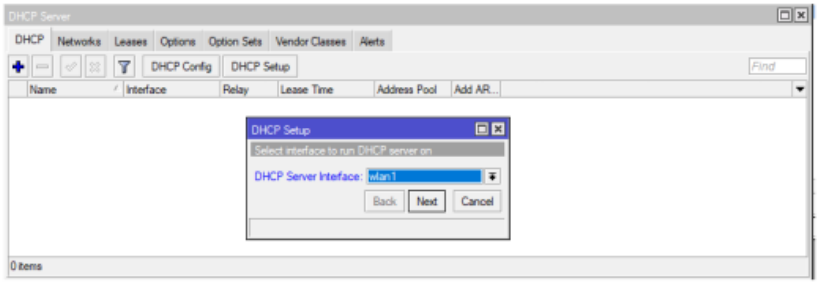


Gambar 6.4. mengisi Route List

Jika sudah, maka statusnya akan "reachable", contoh disini adalah pada eth3, selanjutnya lakukan seting DHCP servernya untuk client yang akan koneksi melalui menu *IP > DHCP server*, misalnya isi interface nya eth2. Setelah itu, di sisi client / antar client coba lakukan ping untuk tes koneksi.



Gambar 6.5. Reachable pada Eth



Gambar 6.6. Seting DHCP server

Administrator harus secara manual menambahkan rute ke semua router apabila ada jaringan / station yang ditambah, apabila skala jaringan termasuk kecil. Routing secara statis tidak cocok untuk jaringan berskala besar karena perlu dikonfigurasi secara manual setiap kali subnet baru ditambahkan, jadi mempertahankannya bisa menjadi pekerjaan penuh waktu yang tidak praktis bagi admin.

BAB VII

QoS (QUALITY OF SERVICE)

QoS bisa didefinisikan sebagai kemampuan jaringan untuk memberikan tingkat jaminan layanan (service) yang berbeda. Di Router OS, bisa diimplementasikan beberapa metode QoS seperti pembatasan lalu lintas traffic, traffic priority, dan lainya. Pengontrolan dan pengelolaan sumber daya jaringan dengan memprioritaskan jenis data tertentu di jaringan bisa dilakukan di QoS. Contohnya, perlunya penyediaan service yang dapat diprediksi dan diskalakan saat aplikasi (seperti suara, video, dan data) melintasi jaringan tarutama pada jaringan di sebuah perusahaan. Mekanisme Queue nantinya yang akan mengelola bagaimana paket mengantri dan akan dikirimkan ke interface adalah bentuk implementasi dari fitur QoS ini.

Queue bekerja ketika aliran paket melewati interface, dimana kita bisa membatasi lalu lintas yang masuk ke router. Kontrol Queue adalah permintaan dan laju pengiriman paket atau data yang melewati interface, menentukan di mana paket menunggu atau dikirim dan yang akan didrop oleh router.

A. Pembatasan Kecepatan (Rate Limit)

Pembatasan dilakukan karena tidak memungkinkan untuk melaksanakan kontrol langsung dari lalu lintas traffic yang masuk, solusinya secara tidak langsung dapat dikendalikan dengan menjatuhkan (drop) paket yang masuk. Ada du acara untuk melakukan pembatasan Rate Limit di Router OS, yaitu :

- CIR (Committed Information Rate)

  Dimana klien akan mendapatkan bandwidth (BW) sesuai dengan batas limit, dengan asumsi bahwa BW yang ada cukup untuk memenuhi CIR semua klien. Jenis ini terjadi saat kondisi bandwith kritis.

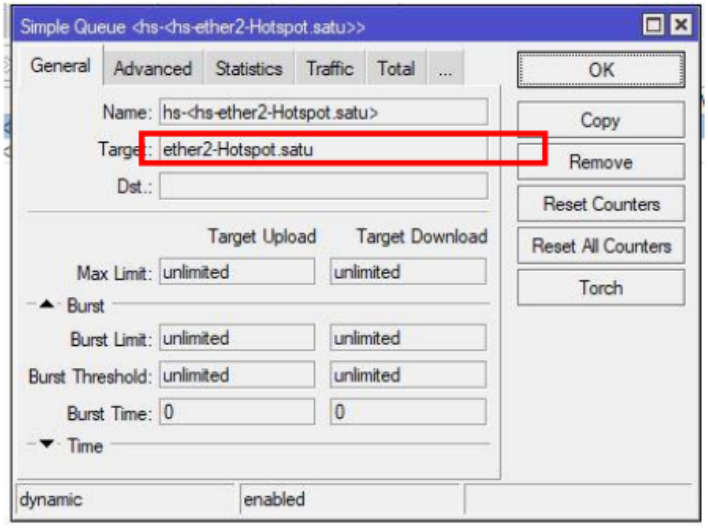
- MIR (Maximal Informatio Rate)

  Akan terjadi jika masih ada sisa BW setelah semua klien mencapai limit, maka terjadilah MIR (Maximum Information Rate) dan

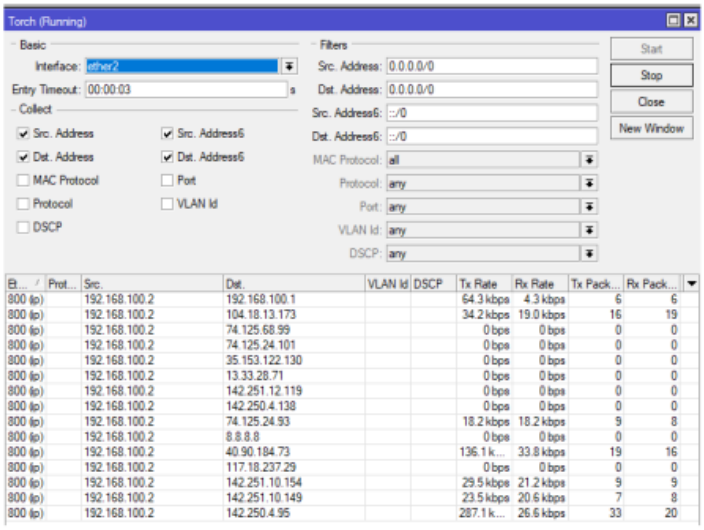
selanjutnya klien bisa mendapatkan tambahan BW hingga batas maksimal tercapai. Limit-at dapat diartikan sebagai bandwidth minimum yang dialokasikan/dialokasikan. Ketika dialokasikan dengan benar, Limit-at adalah bandwidth khusus. Selain itu. Bandwidth minimum yang akan diperoleh jika pembagiannya benar juga pengertian dari Limit-at

B. Queue

Pembatasan bandwidth dapat dilakukan dengan beberapa cara yaitu wireless access list, ppp secret, dan hotspot user pada setiap Router. Menetapkan batas bandwidth dengan hanya mendefinisikan parameter alamat IP (alamat tujuan) dari host atau koneksi yang dibatasi adalah pengertian dari Queue (queue) sederhana. Queue sederhana adalah Queue yang hanya melakukan Maximum Restricted Bandwidth (MIR). Untuk mengkonfigurasinya di Mikrotik, Kita dapat mengakses Queues Menu > Simple Queues > Add. Setelah itu akan muncul status Queue, dan selain itu kita bisa melakukan Toot Torch. Torch adalah alat di Mikrotik untuk melihat bandwidth secara real time dan berapa bandwidth yang digunakan pada setiap komputer. Hal ini memungkinkan kita untuk memantau penggunaan bandwidth setiap komputer di jaringan. Kita dapat menggunakan fungsi ini dengan mengakses pada menu Tools > Torch.



Gambar 7.1. Simple Queue

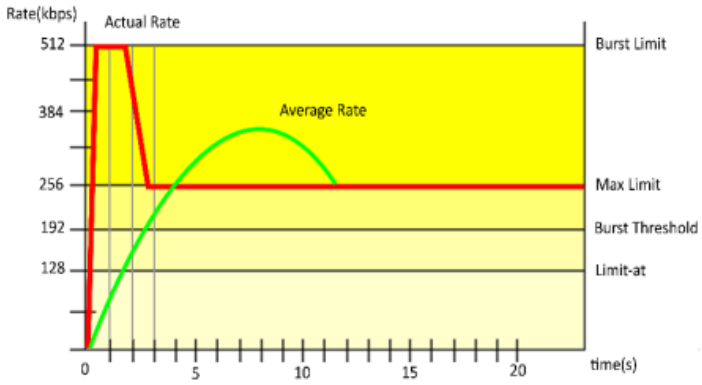


Gambar 7.2. Torch Status

C. Bursting

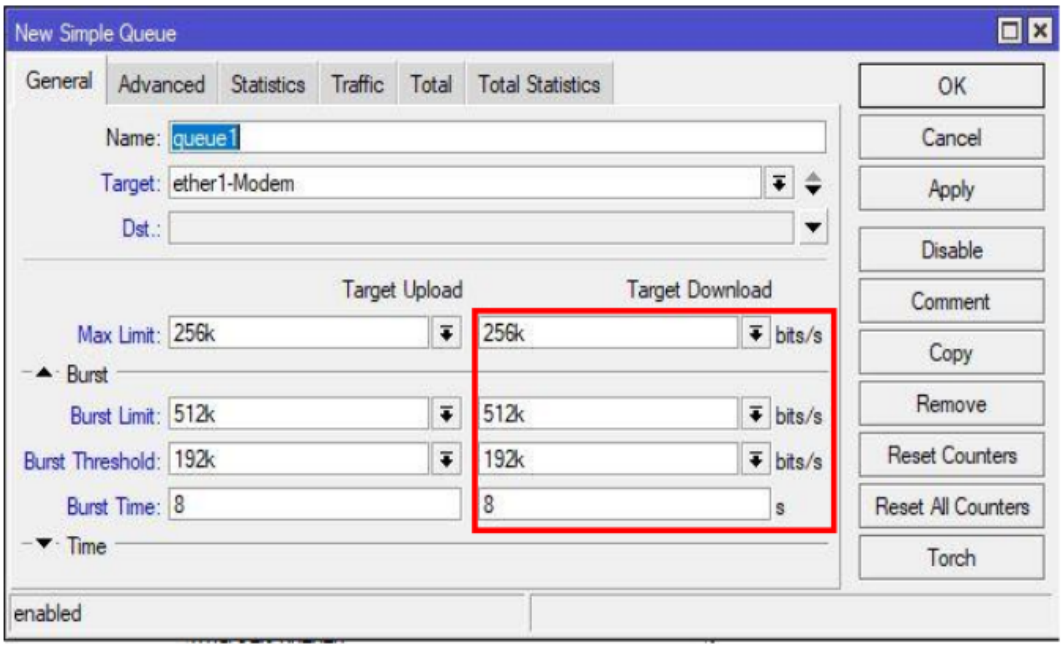
Salah satu cara untuk meningkatkan kinerja koneksi HTTP disebut bursting. Penggunaan metode ini untuk memungkinkan peningkatan kecepatan data dalam waktu yang singkat (burst time). Burst dapat digunakan jika kecepatan data rata-rata kurang dari ambang batas burst, (kecepatan data aktual dapat mencapai batas burst). Kecepatan data rata-rata akan dihitung dari detik terakhir waktu burst.

Sebagai contoh, Brust Limit dengan bentuk Limit-at=128kbps, max-limit=256kbps, burst-time=8,burst- threshold=192kbps, dan burst-limit=512kbps.

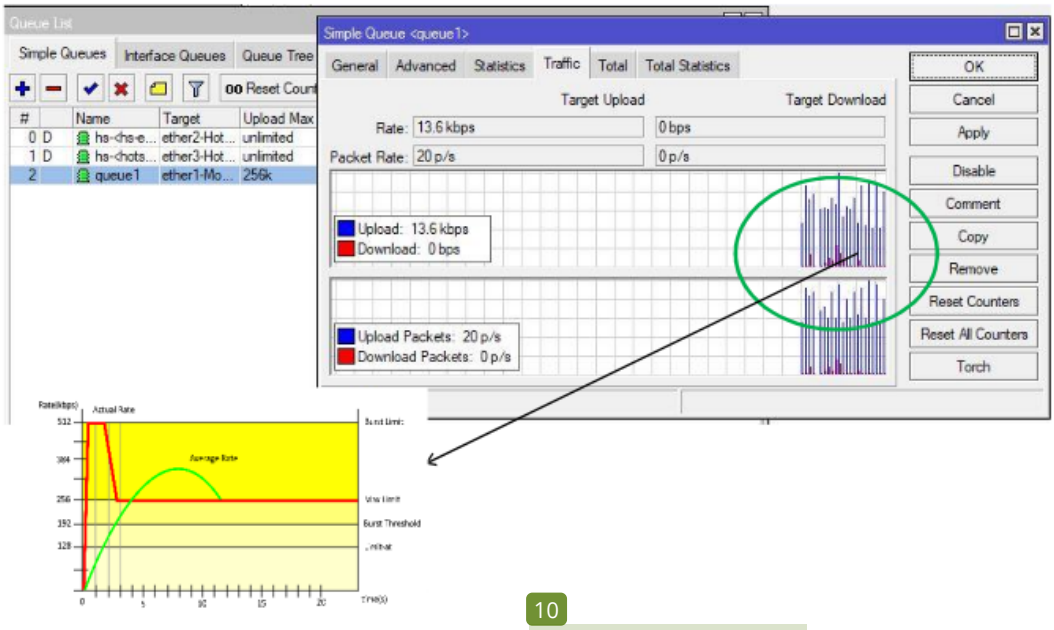


Gambar 7.3. Analogi Burst

Teknik ini dapat digabungkan dengan metode Simple queue, pada contoh di atas kita dapat mengatur menu Queue > Simple > Add New. Untuk melihat trafiknya bisa dilihat di menu Queue>Simple Queue>Traffic.



Gambar 7.4. burst Simple Queue

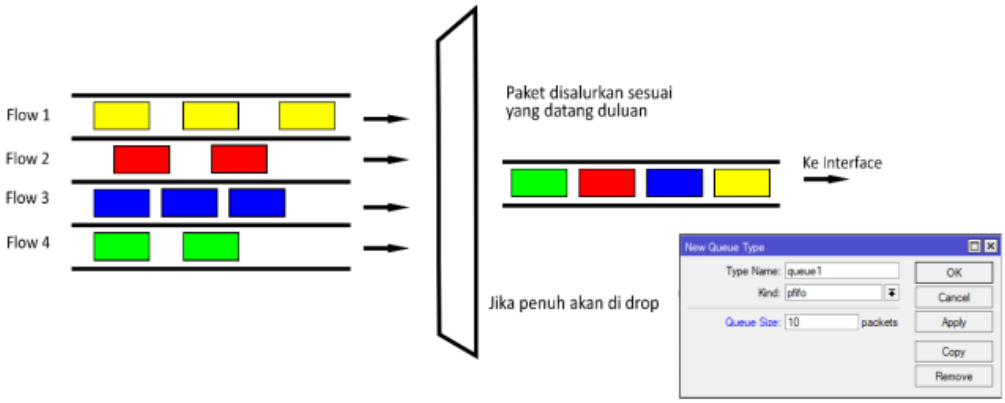


Gambar 7.5. Traffic Burst Simple Queue

D. Jenis Queue

Scheduler yang menggunakan BFIFO atau Bytes First In First Out, PFIFO atau Packets First-In First-Out, RED atau Random Early Detect, SFQ atau Stochastic Fairness Queuing dan yang menggunakan PCQ atau Per Connetion Queue dan HTB atau Hierarki Token Bucket adalah jenis Queue atau queue. Untuk memilih jenis Queue bisa dilihat dan di konfogirasi di menu Queue > Queue Type > Add New. Untuk PFIFO dan BFIFO buffernya lebih kecil karena menggunakan algoritma tipe FIFO. Algoritma tipe ini tidak mengubah urutan paket, hanya menyimpan dan menyalurkan jika memungkinkan. Paket akan dijatuhkan (drop) Jika buffer penuh. Jalur data yang tidak terlalu padat dianjurkan dan cocok untuk menggunaka jenis FIFO.

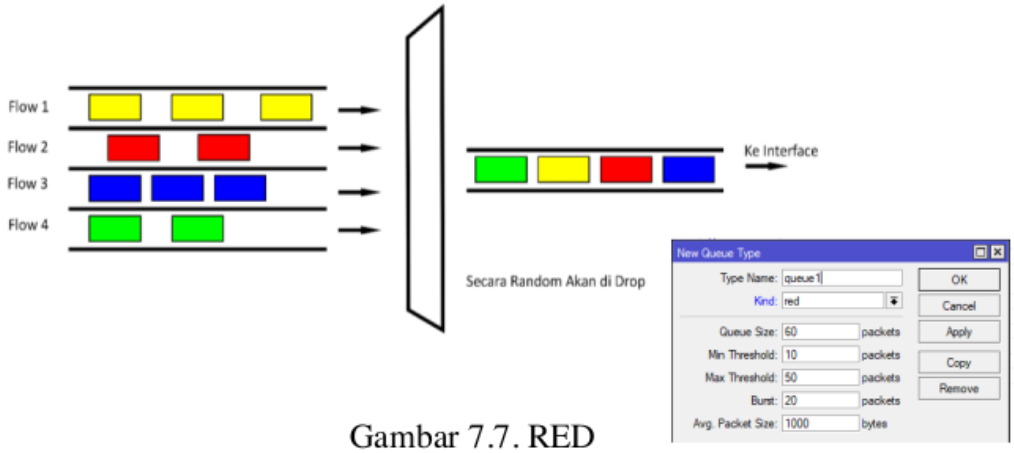
Menentukan jumlah data yang dapat diantrekan di buffer merupakan Parameter "pfifo-limit" dan "bfifo-limit" yang didedikasikan untuk sistem perangkat keras dengan prosesor multi-core dan harus berada pada antarmuka yang mendukung beberapa Queue transmisi disebut MQ-FIFO.



Gambar 7.6. FIFO

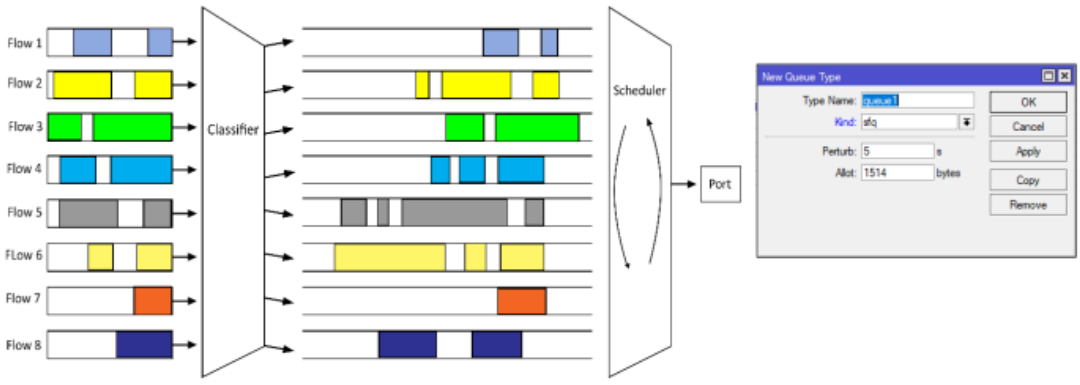
Membatasi paket dengan melihat ukuran Queue rata-rata adalah fungsi dari RED. Ukuran Queue rata-rata dibandingkan dengan dua parameter, ambang batas minimum dan ambang batas maksimum (min dan max threshold) adalah parameter RED. Tidak ada paket yang dijatuhkan (didrop) ketika ukuran queue rata-rata sama dengan ambang minimum. Semua paket yang masuk akan dihapus (drop) Jika ukuran Queue rata-rata melebihi ambang batas maksimum. Ketika ukuran Queue rata-rata berada di

antara ambang batas minimum dan maksimum maka paket dijatuhkan secara probabilistik. Jika ada lalu lintas paket yang padat, jenis queue RED biasanya digunakan karena bagus untuk lalu lintas trafik TCP dan bagus untuk lalu lintas trafik UDP.



Gambar 7.7. RED

Queue sebenarnya tidak tersedia di SFQ karena Hanya menggunakan algoritma hasing untuk mengklasifikasikan paket menjadi 1024 subqueue dengan melihat 4 parameter (src – dst ip address dan src – dst port) dalam metode ini. Algoritma round-robin nantinya yang akan kemudian merequeue/mendistribusikan lalu lintas trafik dari setiap subflow yang ada. Algoritma hasing akan mengubah lalu lintas sesi (session traffic) dan membaginya menjadi subqueue lain dengan sejumlah besar paket..

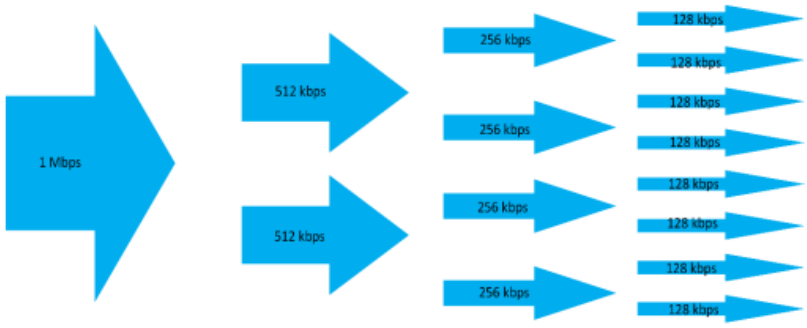


Gambar 7.8. SFQ

Selanjutnya adalah fungsi PCQ (Per Connection Queue) yang bisa diartikan metode manajemen bandwidth yang sangat sederhana karena PCQ menggunakan algoritma yang mendistribusikan bandwidth secara merata ke banyak klien online atau aktif. PCQ idealnya diterapkan jika kita kesulitan mengatur bandwidth per klien. Fitur PCQ ini tidak membatasi jumlah subqueue, namun PCQ membutuhkan memori yang cukup besar dan PCQ merupakan peningkatan dari SFQ.

Untuk mengoptimalkan QoS dengan mengelompokkan aliran data ke dalam sub aliran, maka kita bisa megunakan PCQ ini. Berdasarkan parameter dari pcq-classifier (src-address, dst-address, src-port, dst-port) nanti akan kita buat subqueue. Kecepatan data maksimum (pcq-rate) dan jumlah paket (pcq-limit) per subqueue dapat kita batasi. Di subqueue PCQ tidak boleh melebihi jumlah paket sesuai dengan pcq-total-limit pada total Queue. Metode di PCQ adalah:

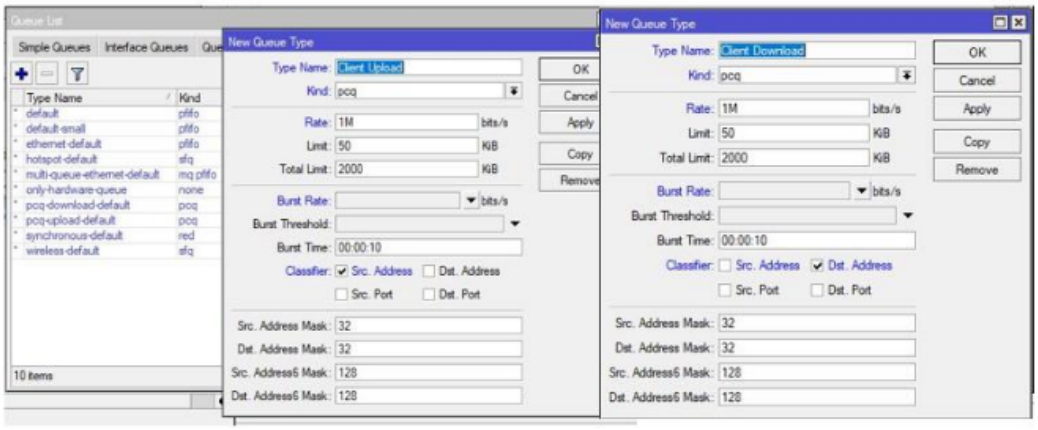
- pcq-rate – membatasi bandwidth maksimum yang dapat diperoleh setiap substream menggunakan metode jenis ini.
- Pcq limit - koneksi yang diizinkan per klien, misalnya 50 koneksi per klien menggunakan metode jenis ini
- Total Limit - Jumlah maksimum data yang diantrekan di semua substream



Gambar 7.9. Ilustrasi PCQ

Sebagai contoh, kita akan membuat PCQ dengan tujuan membatasi kecepatan unduh klien hingga 1Mbps dan kecepatan unggah hingga 1Mbps, dan kita akan mencoba membuat dua jenis Queue baru. Dst Address

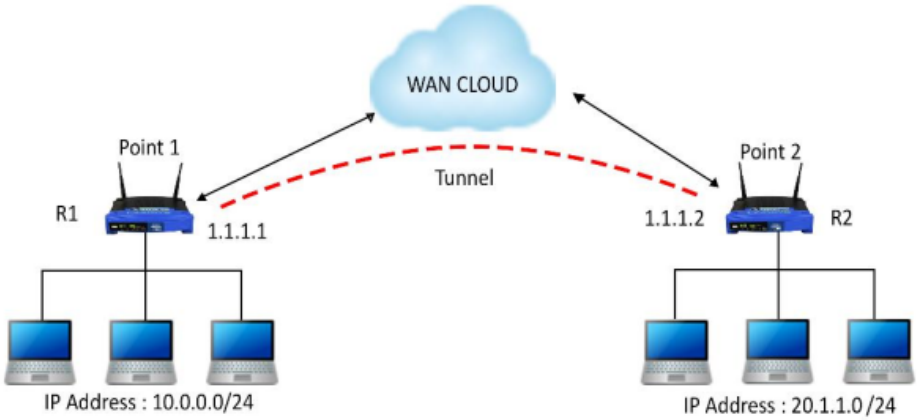
(maksimum download) dan 1 Mbps Src Address (maksimum upload) dengan kecepatan 1 Mbps, selanjutnya kita setting Queue untuk interface LAN dan WAN. Untuk mengkonfigurasi PCQ, kita dapat menggunakan menu Queues > Queues Type > Add. Kita dapat membuat dua PCQ untuk diunduh dan diunggah (upload dan download).



Gambar 7.10. konfigurasi PCQ

BAB VIII
TUNNEL

Tunneling (tunel) dapat didefinisikan sebagai metode menyembunyikan atau mengenkapsulasi paket dalam jaringan. Paket sedikit diubah atau dimodifikasi, yaitu pada header dari tunel yang nantinya akan ditambahkan modifikasi. Ketika data melewati tunnel ke tujuan (ujung), header paket dikembalikan seperti sebelumnya, yang berarti header tunnel akan dihapus.



Gambar 8.1. Ilustrasi Tunnel

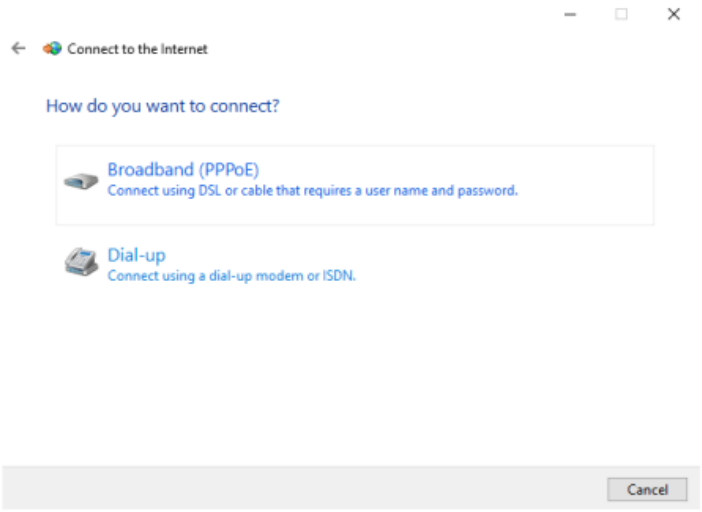
A. Point to Point Protocol (PPP)

Biasanya protocol ini Digunakan untuk membangun sebuah tunnel atau dapat diartikan sebagai koneksi langsung antara dua node adalah pengertian PPP. Metode ini dapat menyediakan otentikasi pada koneksi, enkripsi dan kompresi. Berbagai tunel (tunnel) PPP, seperti PPPoE, SSTP, PPTP, dan lainnya telah didukung oleh Router OS.

1. PPPoE atau Point to Point Protocol over Ethernet,

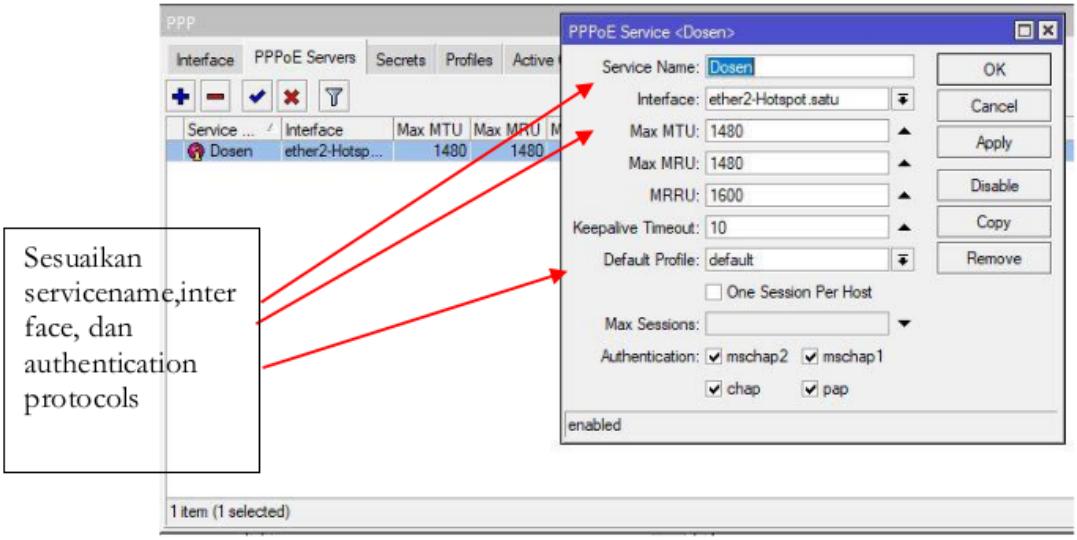
   Merupakan protokol Layer 2 untuk mengenkapsulasi Point-to-Point Protocol (PPP) dalam frame Ethernet. Otentikasi, enkripsi dan kompresi.

PPPoE ini dapat digunakan untuk berbagi alamat IP untuk klien disediakan oleh protocol ini. Klien PPPoE secara default tersedia di hampir semua system operasi, dan Router OS juga mendukung klien PPPoE dan server PPPoE.



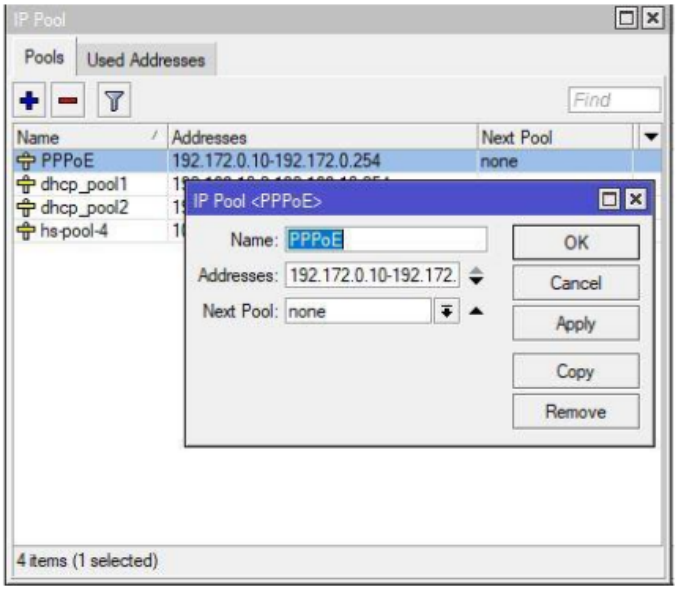
Gambar 8.2. PPPoE Client di Windows

Untuk Membuat PPPoE di Router OS dapat dikonfigurasi di menu PPP > PPPoE Server > Add. Kemudian isikan Service Name dengan nama server PPPoE yang kita inginkan, kemudian pilih Ethernet yang akan digunakan sebagai PPPoE pada interface. Hal ini tidak dapat dikonfigurasi pada antarmuka yang merupakan bagian dari bridge dan Server PPPoE berjalan di salah satu antarmuka (interface). Antarmuka harus dihapus dari keanggotaan Bridge, atau Kita dapat mengatur server PPPoE pada antarmuka bridge jika kita inginkan. Alamat IP tidak boleh digunakan pada antarmuka tempat server PPPoE dikonfigurasi untuk alasan dari segi keamanan.



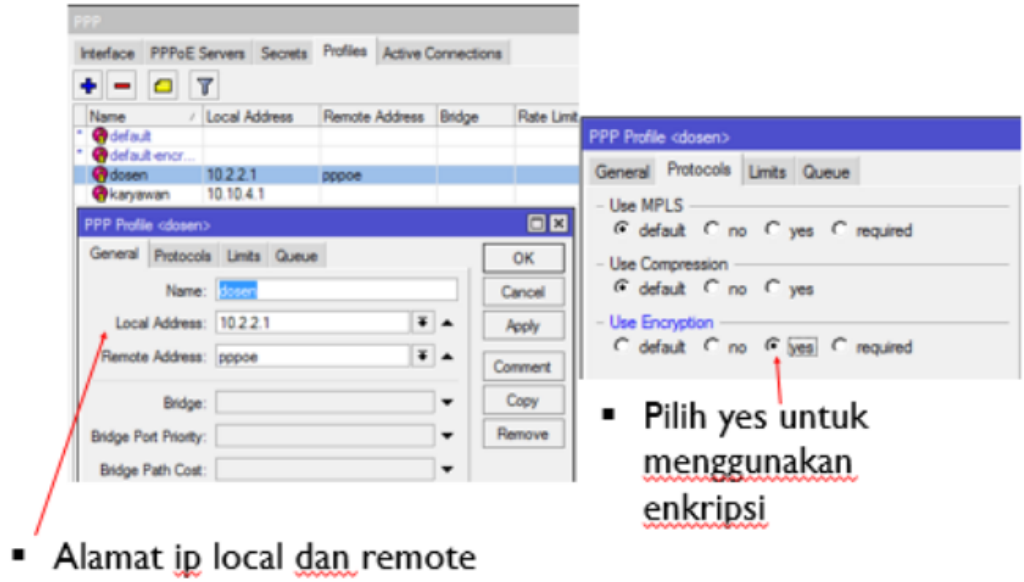
Gambar. 8.3. PPPoE Service

Sebelum mengatur Profile serta Secret, mari kita bisa siapkan IP Pool terlebih dahulu. Dengan cara ini kita tidak perlu menentukan IP yang akan digunakan ketika ada pengguna baru PPPoE. Semuanya akan dikelola oleh kumpulan (pool) IP ini. Untuk menyiapkan kumpulan IP, buka Menu IP > Pool > Add. Masukkan nama pool dan batasan alamat IP.

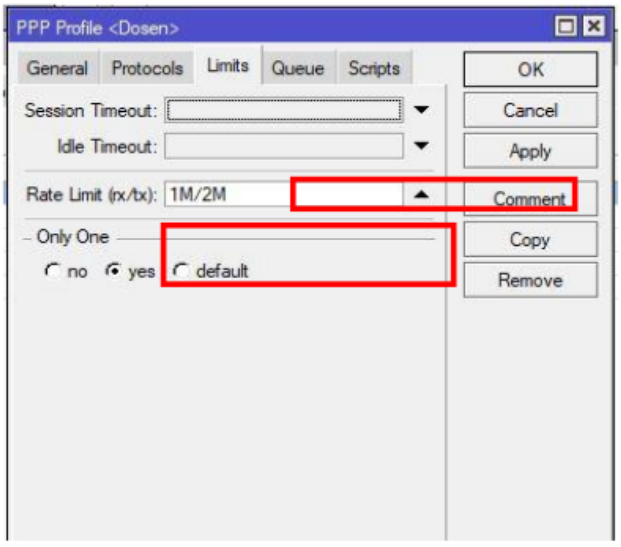


Gambar 8.4. IP Pool

Selanjutnya kita bisa membuat file konfigurasi PPPoE yang menentukan batasan setiap client PPPoE, seperti kecepatan internet, dll. Kita bisa mengaturnya melalui menu PPP > Profiles > Add. Untuk name isikan nama sesuai kebutuhan, untuk local address isikan gateway dari server PPPoE, untuk remote address pilih Ip pool yang kita buat tadi, tetap nilai default bridge learning. Di tab Limit, sesuaikan kecepatan Internet untuk profil. Misalnya kita akan memberikan batas upload 1Mbps dan download 2Mbps, lalu apply/OK.

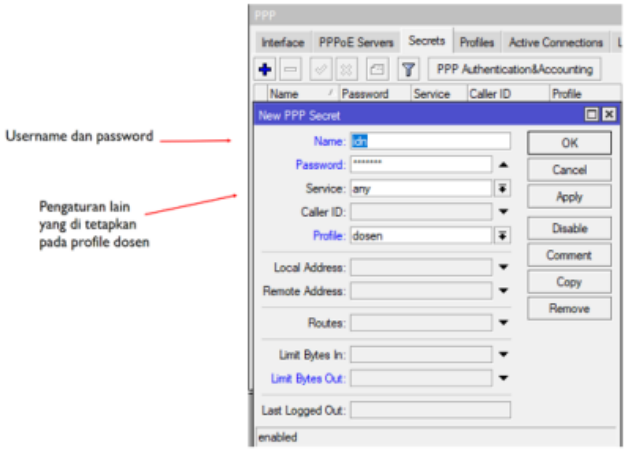


Gambar 8.4 PPP Profile



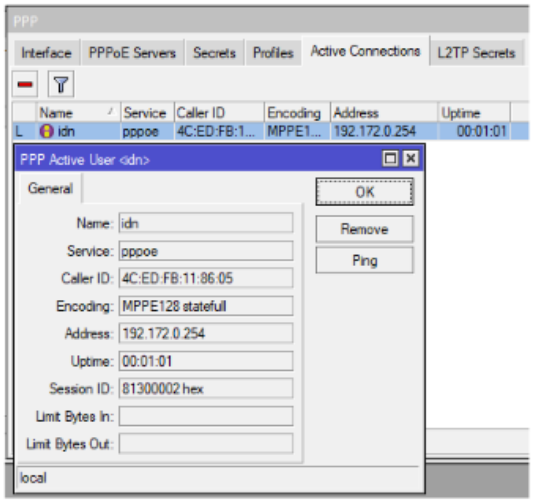
Gambar 8.5. PPP Profile – Limits

Kemudian kita dapat mengatur Secret PPP, yang bertindak sebagai pengguna database untuk klien yang perlu terhubung. Di sini kita dapat mengatur konfigurasi khusus, seperti nama pengguna, kata sandi, dan pengaturan lain. Pada Profil PPP kita bisa melakukan pengaturan lainnya. Pengaturan di file konfigurasi PPP akan cocok dengan di pengaturan di secret PPP



Gambar 8.6. PPP Secret

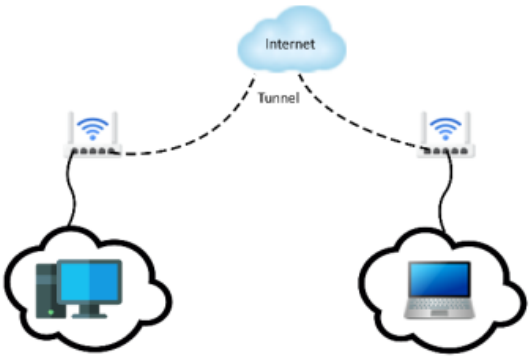
Pada tab *active connection,* kita bisa melihat informsai user yang mengaktifkan dan menggunakan PPP user (PPP Status)



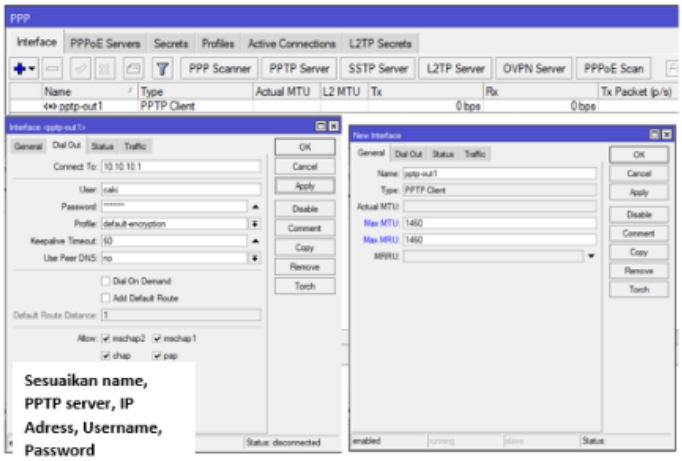
Gambar 8.7. PPP Status

2. PPTP (Point to point Tunnel Protocol),

Pada PPTP, tunel yang banyak digunakan karena hampir semua sistem operasi. Kita perlu memperhatikan pengaturan PPP Secret dan PPP Profiles sebelum menjalankan protokol server PPTP. PPTP di jaringan NAT didukung oleh Helper NAT. Protokol TCP dan GRE (Generic Routing Encapsulation) untuk menyalurkan paket IP ke lapisan tautan data PPP digunakan dalam PPTP. Enkripsi MPPE (Microsoft Point-to-Point Encryption) 40 – 128 bit digunakan dalam metode ini dan PPTP menggunakan port TCP 1723. Menu PPP > Interface > Add di Winbox dipakai untuk mengonfigurasinya terlebih dahulu.

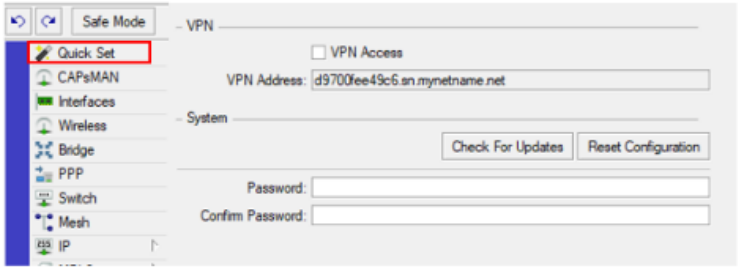


Gambar 8.8. Ilustrasi PPTP Tunnel



Gambar 8.9. Interface PPTP Client

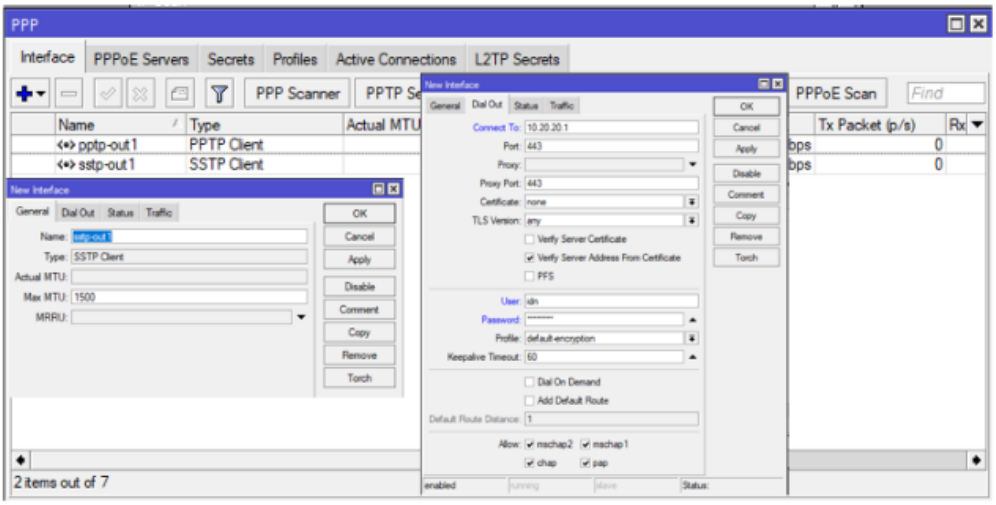
Router OS menyediakan server PPTP sederhana yang dapat kita gunakan untuk keperluan administrasi. Kita dapat menggunakan menu pengaturan cepat (quickset) untuk mengaktifkan akses ke VPN.



Gambar 8.10. PPTP server di menu Quickset

3. SSTP atau Secure Socket Tunnelling Protocol,

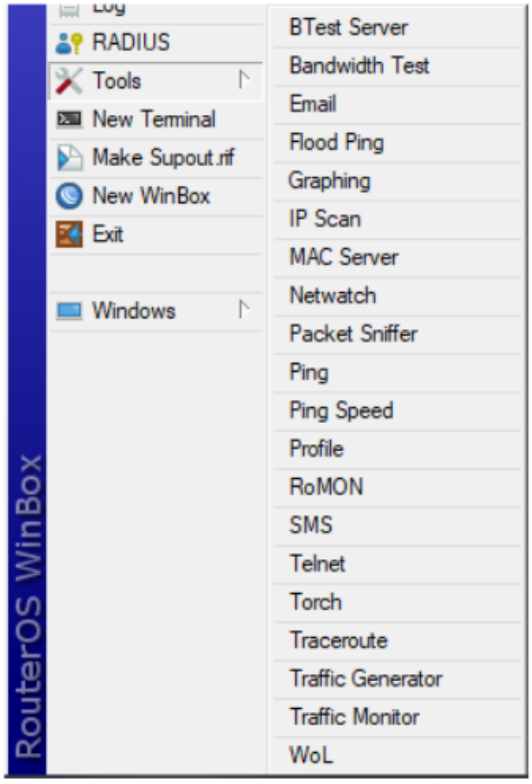
Membuat tunel terenkripsi pada IP menggunakan port tcp / 443 (sama seperti HTTPS) disebut dengan SSTP. Fungsionalitas SSTP klien dan server SSTP didukung oleh Router OS. Di Windows Vista SP1 (dan yang lebih baru) dan edisi lainnya fitur fungsionalitas klien SSTP sudah tersedia. Klien dan server open source dapat diimplementasikan di Linux. SSTP ini adalah trafik yang sama dengan HTTPS dll. SSTP dapat melewati firewall tanpa konfigurasi khusus. Menu > Interface > Add di Winbox dapat dipakai untuk mengatur SSTP ini di PPP. Sesuaikan nama, server SSTP dan alamat IP, nama pengguna dan kata sandi. Untuk mengirim semua lalu lintas melalui tunel SSTP, gunakan Add Default Route serta Untuk mengirim beberapa lalu lintas melalui tunel (tunnel) SSTP menggunakan rute statis. Tidak diperlukan sertifikat SSL untuk menghubungkan antara dua perangkat router *Mikrotik* di SSTP.



Gambar 8.11. SSTP Client

BAB IX
MISC

Pada bagian lainnya (misc) ini, akan membahas beberapa fitur yang ada pada Router OS Mikrotik yang berguna untuk memanajemen dan mengawasi (monitor) Router agar lebih efisien.

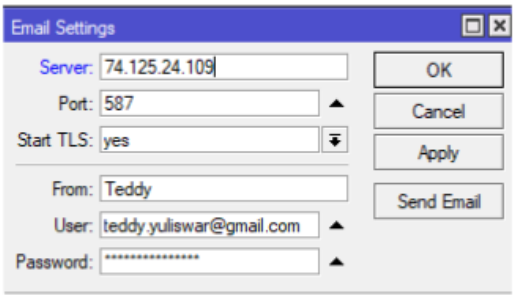


Gambar 9.1. Tools Router OS

A. Tool Manajemen

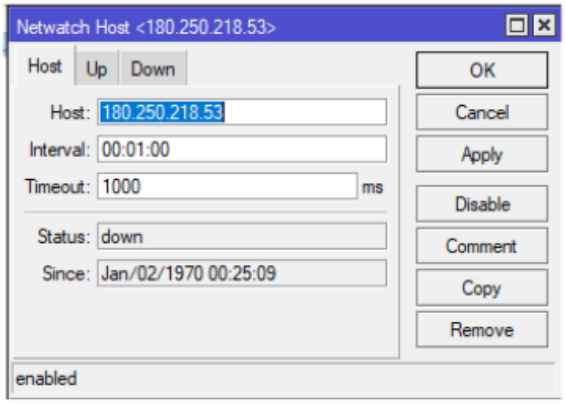
1. Email, misalnya ingin mengirim file backup router, fitur ini memungkinkan kita untuk mengirim email dari router. Setelah mengatur bagian pengaturan email, kita dapat menulis perintah di terminal untuk mengirim email cadangan router. Kita bisa mengisi form, user dan

password dengan email dan password yang kita inginkan. IP server dapat mengisi IP server dalam email.



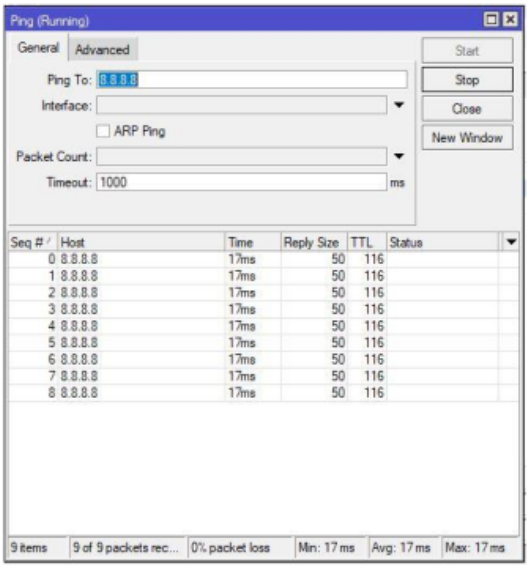
Gambar 9.2. Tool Email.

2. Netwatch, Digunakan untuk memantau status host di jaringan, mengirim ICMP (ping), dan dapat digunakan untuk mengeksekusi skrip saat host menjadi tidak dapat diakses/terjangkau.



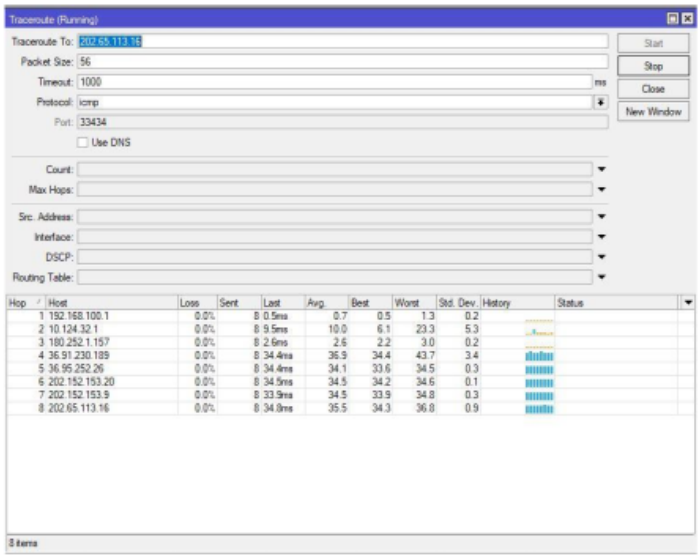
Gambar 9.3. Netwatch

3. Ping, digunakan untuk menguji "jangkauan" host pada jaringan IP dan untuk mengukur waktu perjalanan pulang pergi antara host sumber dan tujuan dan untuk mengirim paket permintaan ICMP bisa menggunakan fitur ini. Misalnya kita melakukan ping ke Google 8.8.8.8



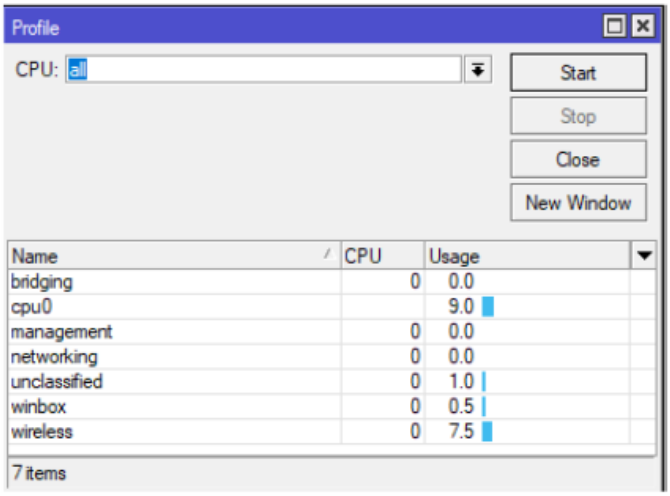
Gambar 9.4. Ping

4. Traceroute (Tracert) yakni Perintah yang menampilkan rute yang ditempuh paket untuk mencapai tujuannya, disebut dengan traceroute. Mengirimkan pesan permintaan Internet Control Message Protocol (ICMP) ke tujuan dengan nilai time-to-live yang meningkat adalah cara yang bisa dilakukan untuk traceroute. Daftar interface router (yang paling dekat dengan host) yang ada pada jalur antara host dan tujuan adalah rute yang ditampilkan di Winbox.



Gambar 9.5. Traceroute

5. Profile, biasanya untuk menampilkan penggunaan CPU dari setiap proses yang berjalan secara real-time pada Router OS bisa dengan menggunakan fitur ini. Selain itu, fitur ini juga bisa menunjukkan idle - sumber daya CPU yang tidak digunakan.

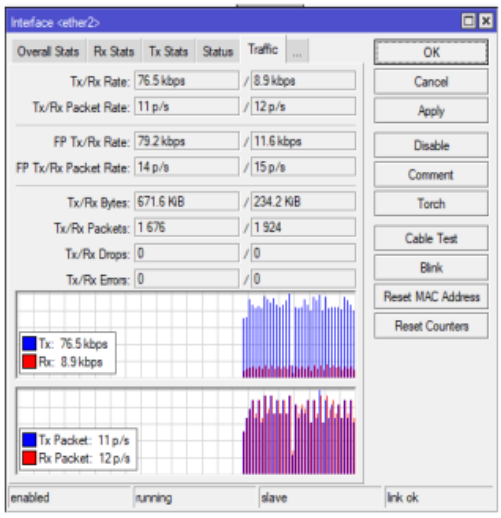


Gambar 9.6. Profile

B. Tools Monitor

1. Interface Traffic Monitor,

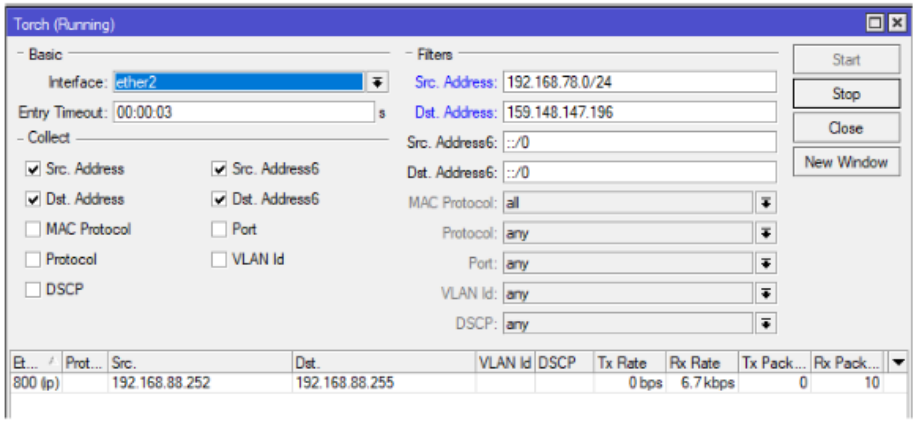
   Memantau kondisi lalu lintas (traffic) secara real time bisa dengan memanfaatkan fitur ini.



Gambar 9.7. Interface Traffic Monitor

2. Torch

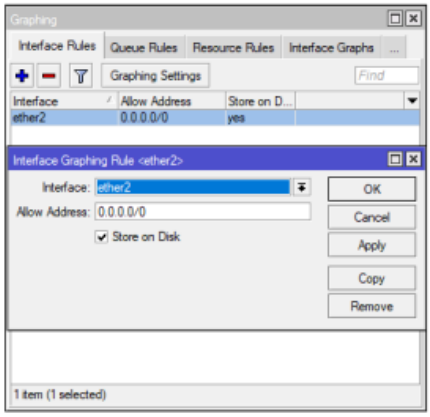
Yakni tool pemantauan jaringan waktu nyata (realtime). Alat ini dapat digunakan untuk memantau lalu lintas yang melewati interface antarmuka. Diklasifikasikan berdasarkan nama IP protokol, alamat sumber/tujuan (IPv4/IPv6), nomor port untuk memantau traffic lalu lintas data.



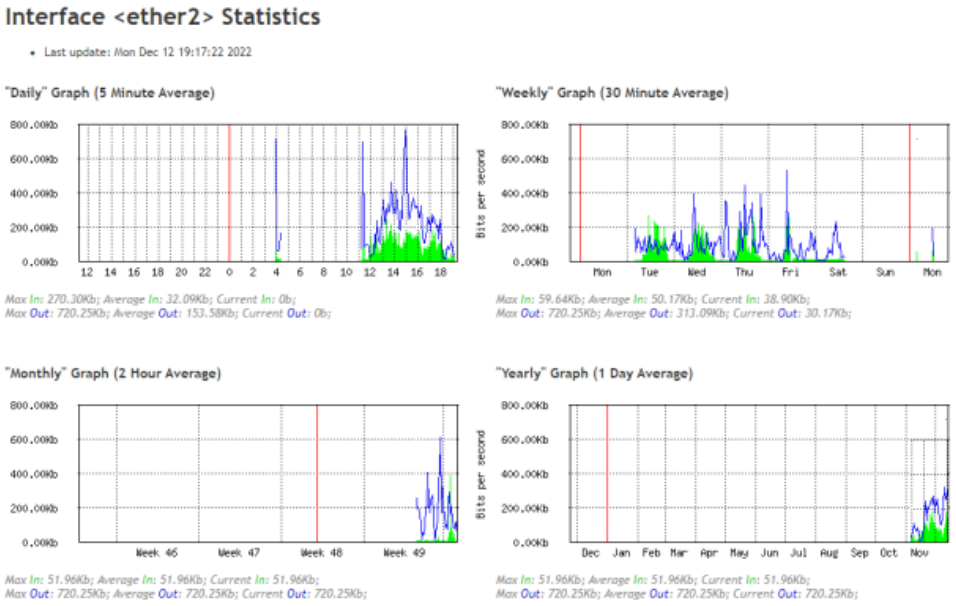
Gambar 9.8. Torch

3. Graphs,

Yakni tool Router OS yang dapat menghasilkan grafik lalu lintas koneksi yang melewati interface atau melihat Queue. Menampilkan penggunaan CPU, memori, dan disk bisa diinformasikan oleh tool ini. Memiliki 4 grafik yaitu harian, mingguan, bulanan, dan tahunan pada tiap metriks. Sesuaikan interfacenya dan ip yang memungkinkan admin untuk melihat grafik sewaktu menggunakannya.



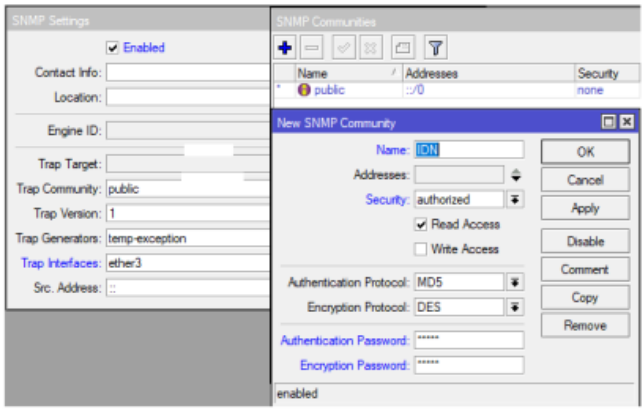
Gambar 9.9. graphs



Gambar 9.10. Statistik Graphs

4. SNMP

   Yaitu Simple network Manajemen Protocol merupakan tool untuk memantau dan mengelola perangkat.

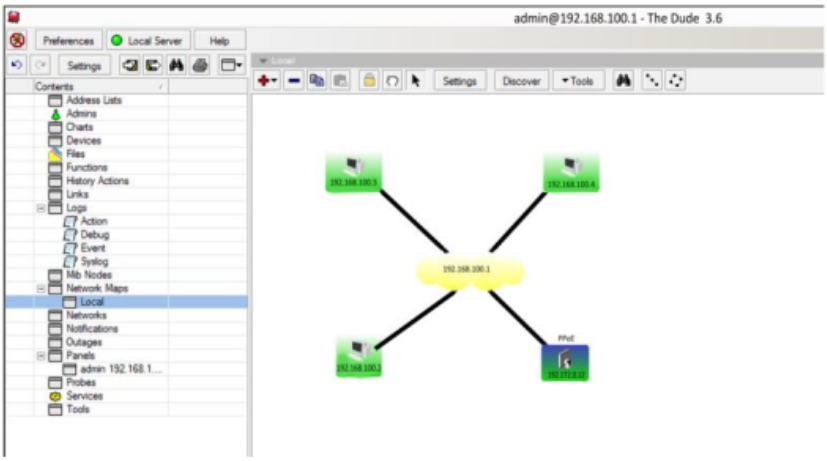


Gambar 9.11. SNMP

5. Dude,

   Digunakan untuk aplikasi dari MikroTik yang secara signifikan dapat meningkatkan cara pengelolaan jaringan. Nantinya alat ini akan memindai semua perangkat dalam subnet tertentu secara otomatis lalu menggambar dan memetakan tata letak jaringan Kita. Alat ini memberi

tahu kita jika ada beberapa beberapa station atau router kita mengalami masalah.



Gambar 9.12. The Dude

PROFIL PENULIS

Indra Laksmana, Lahir di Jambi, 20 Januari 1983. Dosen tetap Program Studi Teknologi Rekayasa Komputer, Jurusan Teknilogi Pertanian Politeknik Pertanian Negeri Payakumbuh, Lulusan Teknik Komputer (S1) UPI dan Ilmu Komputer (S2) di IPB (Institut Pertanian Bogor) Fakultas MIPA departemen Ilmu Komputer. Saat ini menekuni bidang Jaringan Komputer dan Artificial Intelligence.

Syukriadi, Lahir di Padang, 15 Maret 1978. Dosen pada program studi Teknologi Rekayasa Komputer, Jurusan Teknologi Pertanian Politeknik Pertanian Negeri Payakumbuh. Lulusan AMIK YPTK (D3) Sistem Informasi (S1) STMIK Jayanusa dan Ilmu Komputer (S2) UPI YPTK. Saat ini menekuni bidang Jaringan Komputer dan Web Programming

Romy Aulia, Lahir di Padang, 13 Desember 1990. Dosen pada program studi Teknologi Rekayasa Komputer, Jurusan Teknologi Pertanian Politeknik Pertanian Negeri Payakumbuh. Lulusan Teknik Informatika (S1) dan Ilmu Komputer (S2) UPI YPTK. Saat ini menekuni bidang Jaringan Komputer dan GIS

Teddy Yuliswar, Lahir di Padang, 29 Juni 1988. Mikrotik Certified Trainer sejak 2016 setelah mengikuti train-the-Trainer (TTT) Mikrotik di Dubai, Uni Emirate Arab (UEA). Keseharian Sebagai IT Trainer dan Aktif Mengisi Seminar dan Kuliah Umum dan juga Kegiatan Praktisi Mengajar, Bidang Jaringan Komputer dan Keamanan Sistem. Lulusan D3 Politeknik Negeri Padang, S1 STMIK Indonesia Padang dan Sekarang Aktif sebagai Mahasiswa Semester 3 Pada Magister Teknik Elektro Universitas Andalas Padang konsentrasi telekomunikasi. Saat ini menekuni bidang Jaringan Komputer terutama Routing dan Wireless, Cyber Security, Internet of Things (IOT) dan Machine Learning.

jaringan

ORIGINALITY REPORT

21%	21%	1%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pt.slideshare.net Internet Source	4%
2	www.scribd.com Internet Source	2%
3	mikrotik.sar.ac.id Internet Source	2%
4	wiki.mikrotik.com Internet Source	2%
5	www.slideshare.net Internet Source	2%
6	1library.net Internet Source	1%
7	www.coursehero.com Internet Source	1%
8	pdfcoffee.com Internet Source	1%
9	ar.scribd.com Internet Source	1%
10	es.scribd.com Internet Source	1%

11	edoc.pub Internet Source	<1 %
12	id.scribd.com Internet Source	<1 %
13	iritongkos.blogspot.com Internet Source	<1 %
14	qwords.com Internet Source	<1 %
15	bedaliska.wordpress.com Internet Source	<1 %
16	malikagus.blogspot.com Internet Source	<1 %
17	pt.scribd.com Internet Source	<1 %
18	buddy473.blogspot.com Internet Source	<1 %
19	Wahyuni Eka Sari, Muslimin B, Selvia Rani. "Perbandingan Metode SAW dan Topsis pada Sistem Pendukung Keputusan Seleksi Penerima Beasiswa", Jurnal Sisfokom (Sistem Informasi dan Komputer), 2021 Publication	<1 %
20	anwarbuton2.blogspot.com Internet Source	<1 %
21	jaringanakses.wordpress.com Internet Source	<1 %

22	pythonix.biz Internet Source	<1 %
23	id.123dok.com Internet Source	<1 %
24	repository.fatkhan.web.id Internet Source	<1 %
25	m-shohiburridak.blogspot.co.id Internet Source	<1 %
26	anggisr.wordpress.com Internet Source	<1 %
27	informatika.uin-malang.ac.id Internet Source	<1 %
28	debylaadellia.wordpress.com Internet Source	<1 %
29	candramiladre.blogspot.com Internet Source	<1 %
30	Submitted to Universitas Muhammadiyah Surakarta Student Paper	<1 %
31	Submitted to Universitas Muhammadiyah Makassar Student Paper	<1 %
32	nizurholic2004.blogspot.com Internet Source	<1 %
33	nurkamilahaprilia07.blogspot.com Internet Source	<1 %

34	ikee.lib.auth.gr Internet Source	<1 %
35	journal.stmikjayakarta.ac.id Internet Source	<1 %
36	blog.klikcair.com Internet Source	<1 %
37	www.androidponsel.com Internet Source	<1 %
38	anisanoviasari.wordpress.com Internet Source	<1 %
39	blogs.uny.ac.id Internet Source	<1 %
40	core.ac.uk Internet Source	<1 %
41	dickyalkaaffahkpjn.blogspot.com Internet Source	<1 %
42	docplayer.info Internet Source	<1 %
43	ft.unmul.ac.id Internet Source	<1 %
44	id.ipshu.com Internet Source	<1 %
45	repository.radenintan.ac.id Internet Source	<1 %
46	sigernetwork.blogspot.com Internet Source	<1 %

47	sitikomariah07.blogspot.com Internet Source	<1 %
48	walidumar.my.id Internet Source	<1 %
49	wildaida30.blogspot.com Internet Source	<1 %
50	wildanroki.blogspot.com Internet Source	<1 %
51	www.teorikomputer.com Internet Source	<1 %
52	yenkkye.blogspot.com Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		