

Mikrotik

Semester II TA: 2020/2021

S-207



Abstract Class



Class Yang:
- Belum Jadi
- Ngak Komplit
- Ngak Jelas

amun Class dapat dicompile

@pranadana_ | p



Website



Facebook

Mikrotik

Kode Buku: S-207

Revisi ke- 1

Tanggal : 10 Januari 2021

Penulis: Wahyu Januar Alfian

© Hak Cipta Pesantren PeTIK

Materi/diktat/modul ini dilisensikan sebagai **CC BY versi 4.0** sesuai dengan ketentuan lisensi dari **Creative Commons** (<https://creativecommons.org/licenses/by/4.0/deed.id>). Anda diperbolehkan **berbagi** (menyalin dan menyebarkan kembali materi ini dalam bentuk dan format apapun) dan **mengadaptasi** (menggubah, mengubah, dan membuat turunan dari materi ini) untuk kepentingan apapun, termasuk kepentingan komersial, dengan ketentuan sebagai berikut:

- Anda harus mencantumkan (tidak menghapus) pernyataan hak cipta ini;
- Anda harus menyatakan ada perubahan materi jika Anda telah melakukan perubahan; dan
- Ketentuan lain yang terdapat dalam dokumen lisensi CC BY 4.0.

Jika ada sebagian konten materi/diktat/modul ini mengandung karya cipta atau merek dagang pihak lain maka hak cipta atau merek dagang sebagian konten itu tetap menjadi milik masing-masing pihak.

KATA PENGANTAR

Puji syukur kami panjatkan kehadiran Allah SWT, karena dengan rahmat dan karunia-Nya kami dapat menyelesaikan modul Pengantar Sistem dan Jaringan Komputer ini. Sholawat dan salam senantiasa tercurah pada junjungan kita Nabi Muhammad SAW. Modul Mikrotik ini ditujukan untuk pembelajaran para santri di lingkungan Pesantren PeTIK.

Modul ini disusun berdasarkan pengalaman penulis dalam memberikan pengajaran kepada para santri di lingkungan Pesantren PeTIK. Dalam proses pengajaran di kelas, pengajar atau asistennya dapat memberikan tugas tambahan atau latihan atau workshop agar kompetensi santri dapat meningkat secara cepat.

Penulis sangat memahami bahwa apa yang telah di dapatkan selama pembuatan modul belumlah seberapa. Penulis menyadari sepenuhnya bahwa modul ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik yang bersifat membangun sangat penyusun harapkan demi kesempurnaan modul ini. Dan tidak lupa penulis mengucapkan terimakasih kepada semua pihak yang telah membantu penulisan modul ini. Semoga modul ini dapat bermanfaat bagi pembacanya.

Semoga semua usaha yang telah kita lakukan menjadi amal baik yang terus membawa manfaat hingga akhir zaman.

Depok, 10 Januari 2021

Penulis

DAFTAR ISI

KATA PENGANTAR.....	I
DAFTAR ISI.....	II
BAB 1 WEB PROXY SERVER.....	1
1.1 WEB PROXY	1
1.3 TRANSPARENT PROXY.....	5
BAB 2 BRIDGE.....	8
2.1 KONFIGURASI BRIDGE	8
2.2 STP	10
BAB 3 FIREWALL.....	12
3.1 APA YANG DIMAKSUD DENGAN FIREWALL?	12
3.2 TABLE	13
3.3 FILTER	13
3.4 NAT.....	18
3.4.1 Source NAT.....	19
3.4.2 Destination NAT	20
3.5 MANGLE.....	21
BAB 4 VPN.....	24
4.1 VPN.....	24
4.2 PPTP.....	25
4.2.1 Konfigurasi PPTP Server	25
4.2.2 Konfigurasi PPTP Client	29
4.3 EoIP	30
4.3.1 Konfigurasi EoIP.....	31
BAB 5 HOTSPOT	34
5.1 HOTSPOT.....	34

5.2	KONFIGURASI HOTSPOT	34
5.3	WALLED-GARDEN	36
5.4	IP WALLED-GARDEN	37
BAB 6	QOS.....	39
6.1	QoS	39
6.2	PRINSIP PEMBATAHAN KECEPATAN.....	40
6.3	SIMPLE QUEUES	41
BAB 7	ROUTING	43
7.1	KONSEP ROUTING	43
7.2	TABEL ROUTING.....	45
7.3	ROUTING STATIC	50
7.4	ROUTING DYNAMIC.....	53
7.4.1	ROUTING RIP	53
7.4.2	ROUTING OSPF.....	59
7.4.2.1	Konfigurasi Routing OSPF – Back Bone Area.....	60
7.4.3	ROUTING BGP.....	63
DAFTAR PUSTAKA.....		70

Bab 1

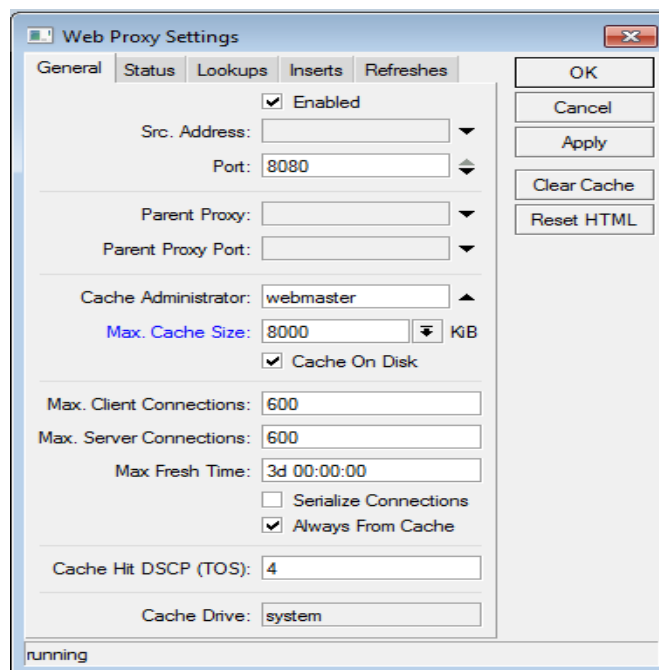
Web Proxy Server

Tujuan:

- Mahasantri mengetahui kegunaan dari web proxy
- Mahasantri mengetahui cara memfilter situs-situs web yang dilarang
- Mahasantri mengetahui cara melakukan transparent proxy

1.1 Web Proxy

Web proxy berfungsi melakukan cache objek-objek internet dengan menyimpan objek yang diminta dari internet, yaitu data yang tersedia melalui protokol HTTP dan FTP pada sebuah sistem yang “dekat” dengan penerima daripada sistem dimana data tersebut berasal. Dekat disini berarti jalur koneksi yang lebih terjamin atau kecepatan akses yang lebih cepat atau keduanya. Web browser kemudian dapat menggunakan cache proxy local untuk mempercepat akses dan mengurangi konsumsi bandwidth. Ketika mengatur server proxy, pastikan server hanya menerima permintaan dari client Anda saja dan tidak disalahgunakan



Gambar 1 Konfigurasi untuk mengaktifkan web proxy

untuk me-relay. Selain itu juga proxy dapat difungsikan untuk memfilter situs-situs atau file yang diakses di internet.

Untuk melakukan konfigurasi web proxy langkah-langkahnya sebagai berikut:

1. Klik IP → Web Proxy → kemudian klik Web Proxy Settings
2. Untuk mengaktifkan centang pada Enabled. Pada Port masukkan port jaringan yang digunakan oleh proxy server untuk menerima permintaan klien. Max Cache Size merupakan besar cache maksimal yang bisa digunakan oleh proxy server. Kemudian klik OK. Sesuaikan Max Cache Size dengan besar media penyimpanan yang Anda miliki.

Untuk konfigurasi command linanya:

```
[admin@MikroTik] > /ip proxy set enabled=yes port=8080 max-cache-size=8000
```

1.2 Access List

Access digunakan untuk memfilter akses client ke internet, dengan membatasi ijin akses ke internet. Access List dikonfigurasi seperti rule firewall biasa. Rules diproses dari atas ke bawah. Rule pertama yang sesuai dengan pengaksesan yang dilakukan akan menentukan apa yang dilakukan dengan koneksi tersebut. Terdapat 6 klasifikasi yang dapat dicocokkan dengan koneksi yang dilakukan. Jika tidak ada klasifikasi yang dispesifikasikan, maka rule tertentu akan sesuai dengan semua koneksi. Jika koneksi sesuai dengan salah satu rule, property action yang dispesifikasi pada rule tersebut akan menentukan apakah koneksi tersebut diperbolehkan atau tidak. Jika tidak ada koneksi tertentu yang sesuai dengan suatu rule maka akan koneksi akan diperbolehkan.

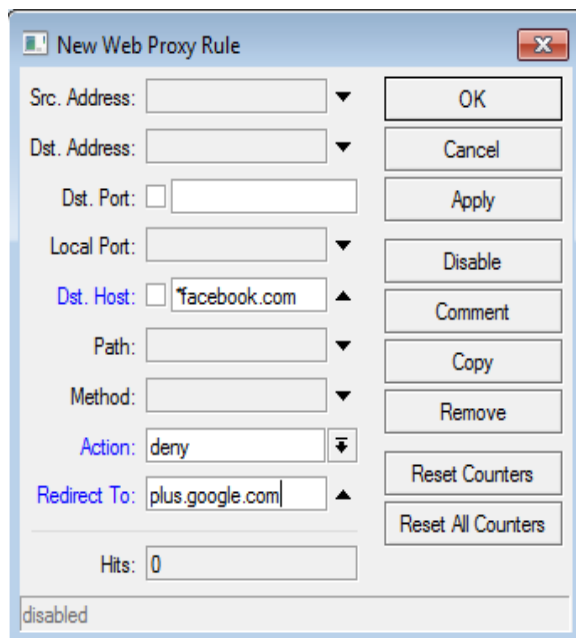
Klasifikasi rule pada Access List:

- Src-address, adalah asal IP address
- Dst-address, adalah IP address tujuan
- Dst-port, adalah port tujuan
- Dst-host, adalah domain atau hostname yang dituju..
- Path, adalah path ke file dalam URL
- Method, adalah method HTTP yang digunakan.

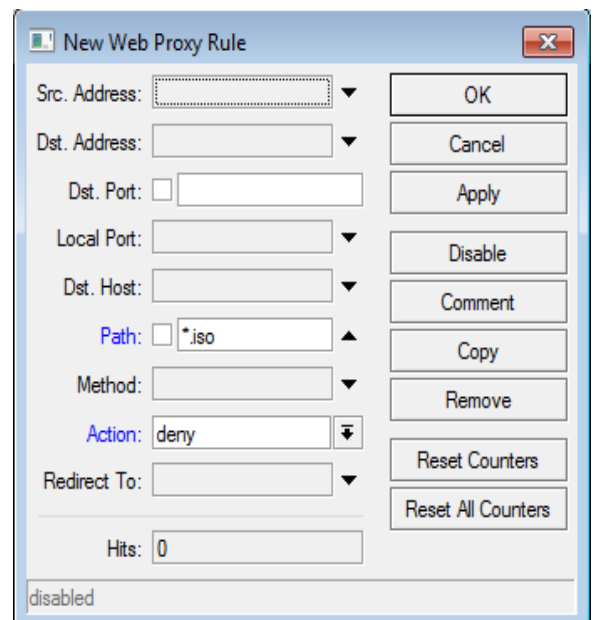
Dalam pengaturan konfigurasi access list urutan berpengaruh pada aturan yang diberikan. ACL yang diletakkan di atas akan menurunkan rutenya ke ACL dibawahnya.

Berikut langkah-langkah konfigurasi ACL pada web proxy server:

1. Klik IP → Web Proxy. Kemudian klik tombol +.
2. Misalkan Anda hendak memblokir situs facebook.com dan pengunduhan file *.iso maka urutan rule yang diberikan sebagai berikut:
 1. Memblok situs facebook.com dengan mengarahkan ke situs plus.google.com.
 - Dst Host: *facebook.com
 - Action: deny
 - Redirect To: plus.google.com
 2. Memblok pengunduhan file dengan ekstensi *.iso.
 - Path: *.iso
 - Action: deny



Gambar 2 Pemblokiran pengunduhan facebook.com



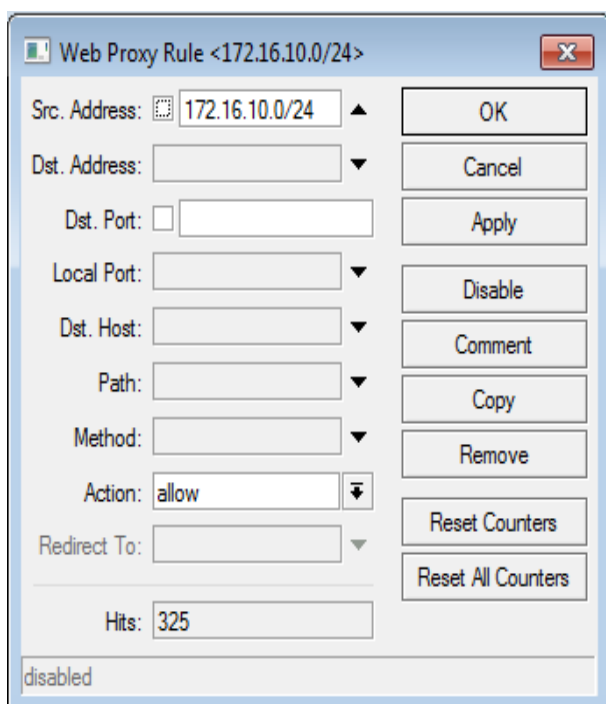
Gambar 3 Konfigurasi pemblokiran File *.iso

3. Memperbolehkan akses untuk client pada jaringan 172.16.10.0/24.

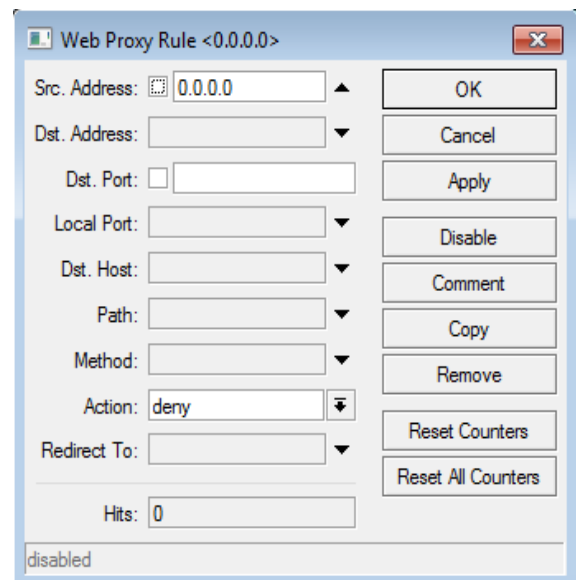
- Src Address: 172.16.10.0/24
- Action: allow

4. Memblokir semua akses.

- Src Address: 0.0.0.0/0
- Action: deny



Gambar 4. Pemberian Akses untuk komputer di LAN



Gambar 5 Pemblokiran semua koneksi

Konfigurasi di command line:

```
[admin@MikroTik] > /ip proxy access add dst-host=*facebook.com action=deny redirect-to=plus.google.com
```

```
[admin@MikroTik] > /ip proxy access add path=*.iso action=deny
```

```
[admin@MikroTik] > /ip proxy access add src-address=172.16.10.0/24 action=allow
```

```
[admin@MikroTik] > /ip proxy access add src-address=0.0.0.0/0 action=deny
```

```
[admin@MikroTik] > /ip proxy access print
```

#	DST-PORT	DST-HOST	PATH	METHOD	ACTION	HITS
0			*.iso	deny	2	
1		*facebook.com		deny	7	
2				allow	292	
3				deny	0	

1.3 Transparent Proxy

Ketika user menggunakan suatu proxy maka pada browser harus dilakukan konfigurasi untuk mengarahkan ke IP address server dan port proxy. Apabila Anda memiliki jumlah client yang cukup besar maka proses penggantian konfigurasi pada browser menjadi proses yang merepotkan. Untuk itu Anda bisa menggunakan transparent proxy untuk mempermudah proses ini.

Konfigurasi transparent proxy ini dilakukan pada router Anda. Cara kerjanya adalah dengan mengarahkan ulang paket ke port web ke port web proxy server. Perlu dipahami bahwa transparent proxy ini hanya berlaku untuk port web (port 80) saja, dan tidak berlaku untuk aplikasi jaringan yang lain. Untuk melakukan pengarahannya digunakan fasilitas dari firewall yaitu NAT.

Konfigurasi transparent proxy sebagai berikut:

1. Klik IP → Firewall → pilih tab NAT. Kemudian klik tombol +.
2. Pada tab General masukkan konfigurasi berikut:
 - Chain: dstnat
 - Src Address: 172.16.10.0/24 (nomor jaringan untuk LAN – optional)
 - Dst Address: 0.0.0.0/0 (mengarah ke IP address manapun atau internet – optional)
 - Protocol: 6(tcp)
 - Dst Port: 80 (port jaringan untuk web)

- In Interface: bridge1 (interface yang terhubung ke LAN)

Gambar 6 Konfigurasi Firewall untuk Tranparent Proxy 1

3. Pilih tab Action dan masukkan konfigurasi berikut:

Gambar 7 Konfigurasi Transparent Proxy 2

- Action: redirect
- To Ports: 8080 (port dari proxy server)

Konfigurasi dari command line:

```
[admin@MikroTik] > /ip firewall nat add chain=dstnat src-address=172.16.10.0/24  
dst-address=0.0.0.0/0 protocol=tcp port=80 in-interface=bridge1 action=redirect to-ports=8080
```

BAB 2

Bridge

Tujuan:

- Mengetahui yang dimaksud dengan interface bridge.
- Mahasantri dapat melakukan konfigurasi bridge.
- Mahasantri dapat melakukan pengaturan bridge agar tidak terjadi looping dalam jaringan.

2.1 Konfigurasi Bridge

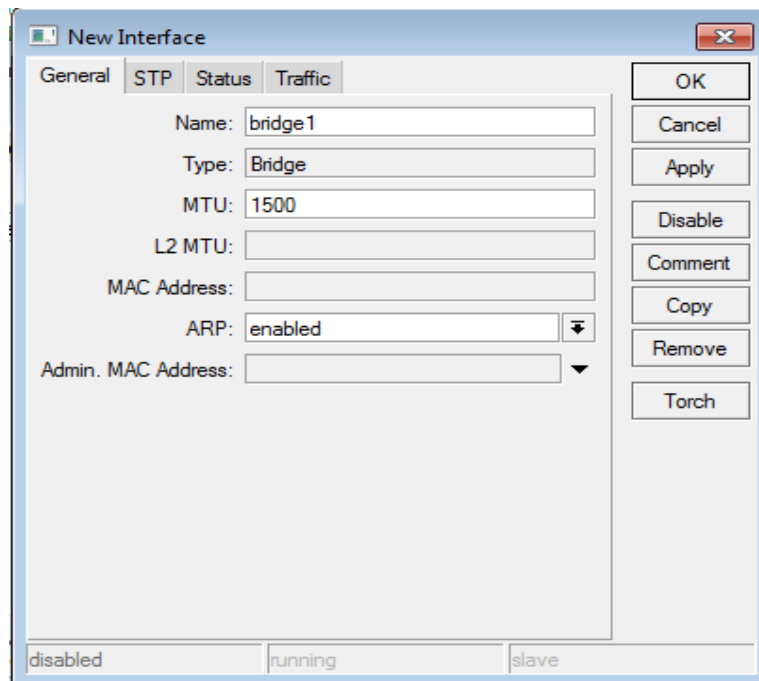
Interface jaringan seperti Ethernet (ethernet, EoIP [Ethernet over IP], IEEE802.11 pada mode ap-bridge atau bridge, WDS, VLAN) dapat dihubungkan menjadi satu dengan menggunakan bridge MAC. Fitur dari bridge memperbolehkan interkoneksi dari host-host terhubung ke LAN yang terpisah, seakan-akan mereka dihubungkan pada satu LAN. Dikarenakan bridge bersifat transparan, maka interface ini tidak akan tampil pada daftar traceroute, dan tidak ada alat yang bisa membedakan antara host yang bekerja pada LAN yang sama dan host yang bekerja pada LAN yang lain apabila LAN ini dibuat menjadi bridge, walaupun bergantung dengan bagaimana LAN dihubungkan maka latensi alat dan kecepatan transfer antar host dapat berbeda-beda.

Untuk menyatukan beberapa interface menjadi satu bridge, sebuah interface bridge harus dibuat, kemudian semua interface dikonfigurasi untuk menjadi port-portnya. Satu MACaddress akan diberikan untuk semua interface di dalam bridge, dalam hal ini MAC address yang terkecil akan dipilih secara otomatis.

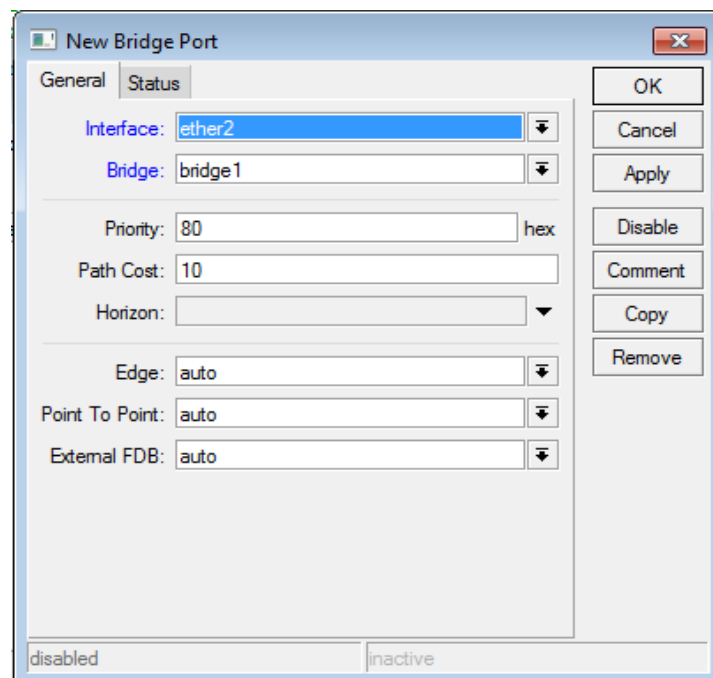
Langkah-langkah pembuatan bridge sebagai berikut:

1. Klik tombol Bridge, kemudian pilih tombol +.
2. Masukkan nama bridge dan klik OK.
3. Kemudian klik tab Ports untuk mendaftarkan port-port network interface sebagai bagian dari interface bridge. Untuk menambahkan tekan tombol +.
4. Pada Interface masukkan network interface yang hendak Anda gabungkan ke dalam

interface bridge. Dan pada bridge Anda masukan nama bridge yang telah Anda buat. Misalkan interface ether2 digabungkan ke dalam bridge dengan nama bridge1.



Gambar 8 Pembuatan Interface Bridge



Gambar 9 Menggabungkan Network Interface ke dalam Bridge

Perintah Command Linenya:

```
[admin@MikroTik] > /interface bridge add name=bridge1
```

```
[admin@MikroTik] > /interface bridge port add interface=ether2 bridge=bridge1
```

2.2 STP

Dengan membuat beberapa interface router Mikrotik Anda sebagai bridge, maka router Mikrotik bertindak seakan-akan sebagai switch. Sama seperti switch, interface tidak harus memiliki IP address. Anda masih bisa memberikan IP address untuk interface bridge, tetapi bukan pada masing-masing interface melainkan di interface bridge itu sendiri.

Sama seperti switch maka bridge akan melakukan pengecekan MAC address perangkat yang terhubung ke masing-masing port dan memasukkannya ke dalam tabel ARP. Oleh karena itu permasalahan yang sama akan terjadi pada bridge apabila terdapat dua kabel jaringan terhubung ke router pada interface-interface bridge kemudian dihubungkan ke switch. Akibat dari tindakan ini adalah terjadinya inkonsistensi ARP table sehingga menyebabkan looping,

Untuk mengatasi hal tersebut router Mikrotik dan switch harus sama-sama menjalankan suatu algoritma yang akan menghitung bagaimana suatu loop dapat dicegah. STP dan RSTP menyebabkan bridge dapat berkomunikasi satu sama lain, sehingga mereka dapat saling bernegosiasi untuk mendapatkan topologi bebas loop. Jalur alternatif yang dapat menyebabkan terjadinya loop dibuat dalam keadaan standby, sehingga pada saat koneksi utama putus, koneksi lain dapat menggantikan. Oleh karena itu protokol ini akan menyebabkan koneksi menjadi redundant.

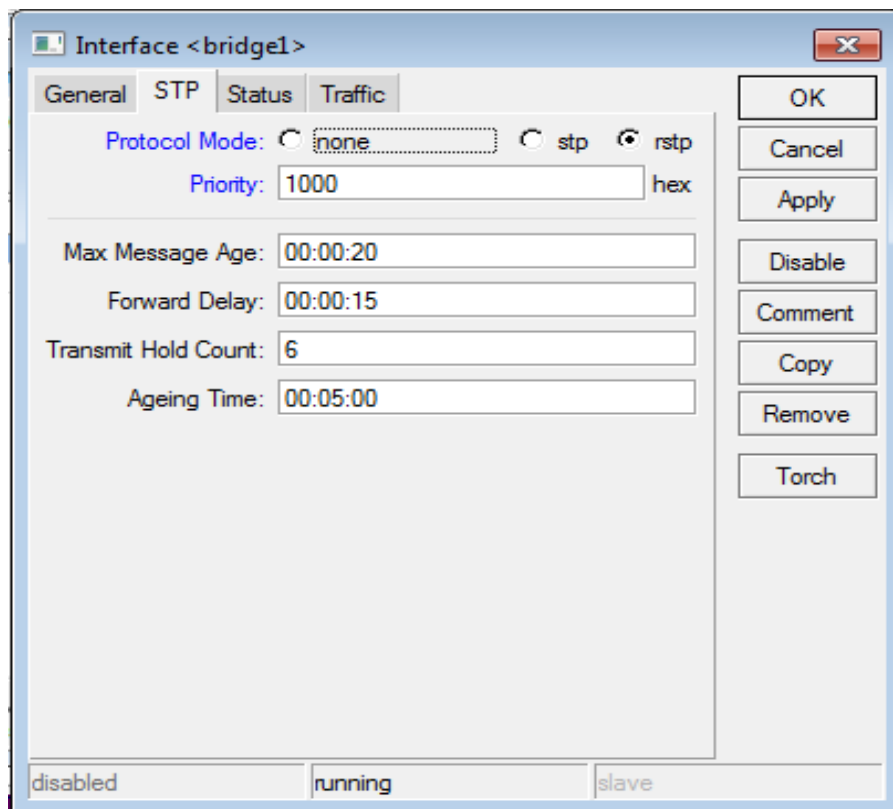
Algoritma ini akan saling bertukar konfigurasi (BPDU – Bridge Protocol Data Unit) secara periodik, sehingga semua bridge akan selalu terbaharui dengan informasi terbaru tentang perubahan pada topologi jaringan. STP akan memilih root bridge yang bertanggung jawab untuk rekonfigurasi jaringan, seperti melakukan pemblokiran dan pembukaan port dari bridge yang lainnya. Root bridge dipilih berdasarkan bridge ID yang terendah. Dalam RouterOS bridge ID ditentukan dengan priority. Priority berupa angka dari 0 hingga 65535, sedangkan default priority dalam Mikrotik adalah 32768. Bila kedua device bridge memiliki priority yang sama, maka penentuan root bridge dengan menggunakan MAC address terendah.

Pada RouterOS terdapat dua protokol STP, yaitu STP dan RSTP. Protokol RSTP (Rapid

STP) memiliki fungsi yang sama dengan STP, yaitu membentuk topologi bebas loop, tetapi RSTP memberikan pembentukan kembali spanning tree yang lebih cepat ketika terjadi perubahan topologi jaringan. Perubahan topologi terjadi ketika jalur utama koneksi putus atau mati.

Untuk melakukan konfigurasi STP langkahnya sebagai berikut:

1. Klik Bridge → klik dua kali pada salah satu bridge
2. Pilih tab STP
3. Kemudian pilih rstp pada Protocol Mode dan masukkan pada Priority bridge ID yang Anda inginkan. Bridge ID akan bertindak sebagai root bridge. Pada Priority



Gambar 10 Pengkonfigurasi STP pada Bridge

menggunakan bilangan heksadesimal. Jadi bila Anda isi dengan 1000 maka nilai desimalnya adalah 4096

4. Lakukan langkah ini di kedua device bridge dengan bridge ID yang berbeda.

BAB 3

Firewall

Tujuan:

- Mengetahui apa yang dimaksud dengan firewall
- Mahasantri dapat melakukan filtering paket dengan firewall
- Mahasantri Dapat mengetahui cara menggunakan NAT pada firewall

3.1 Apa yang dimaksud dengan Firewall?

Firewall mengimplementasi paket filtering dan oleh karena itu menyediakan fungsi sekuriti yang digunakan untuk mengelola arus data dari, ke dan melewati router. Bersama dengan Network Address Translation (NAT) firewall bertugas sebagai alat untuk mencegah akses yang tidak berhak ke jaringan yang terkoneksi secara langsung dan router itu sendiri serta memfilter untuk lalu lintas jaringan ke luar.

Firewall menjaga data-data yang sensitif yang berada di dalam jaringan dari ancaman dari luar. Kapan pun jaringan lain dihubungkan, selalu ada ancaman bahwa seseorang dari luar jaringan Anda hendak membobol masuk jaringan LAN Anda. Pembobolan seperti ini dapat menyebabkan data-data rahasia dicuri dan disebarkan, data-data berharga diubah atau dihancurkan, atau keseluruhan harddisk dihapus. Firewall digunakan untuk tujuan mencegah atau meminimalisir resiko keamanan yang diakibatkan hubungan ke jaringan yang lain. Firewall yang dikonfigurasi dengan baik memainkan peranan penting dalam pembentuk infrastruktur jaringan yang efisien dan aman.

Mikrotik RouterOS memiliki implementasi firewall yang sangat bagus dengan fitur-fitur berikut:

- Pengecekan status packet
- Pendeteksian protokol layer-7
- Filtering protokol peer-to-peer
- Klasifikasi lalu lintas jaringan berdasarkan:

- Asal MAC address
- IP addresses (berdasarkan nomor jaringan atau kelompok IP) dan tipe pengalamaan (broadcast, local, multicast, unicast)
- port dan jangkauan port
- Protokol IP
- Opsi protokol (tipe ICMP and code fields, TCP flags, IP options dan MSS)
- Interface tempat paket datang atau pergi
- internal flow dan connection marks
- DSCP byte
- Isi paket
- Kecepatan pada saat paket datang dan sequence numbers
- Besar paket
- Waktu kedatangan paket
- dll

3.2 Table

Firewall dalam RouterOS dibedakan menjadi beberapa macam fungsionalitas, setiap fungsi ini dibedakan dalam bentuk table. Yaitu:

- Table filter, digunakan untuk memblokir paket-paket yang masuk, keluar atau melewati router.
- Table NAT (Network Address Translation), digunakan untuk melakukan perubahan tujuan atau asal dari suatu paket jaringan.
- Table mangle, menandai paket tertentu (flagging) paket dari jaringan untuk keperluan aplikasi yang lain, seperti QoS.

3.3 Filter

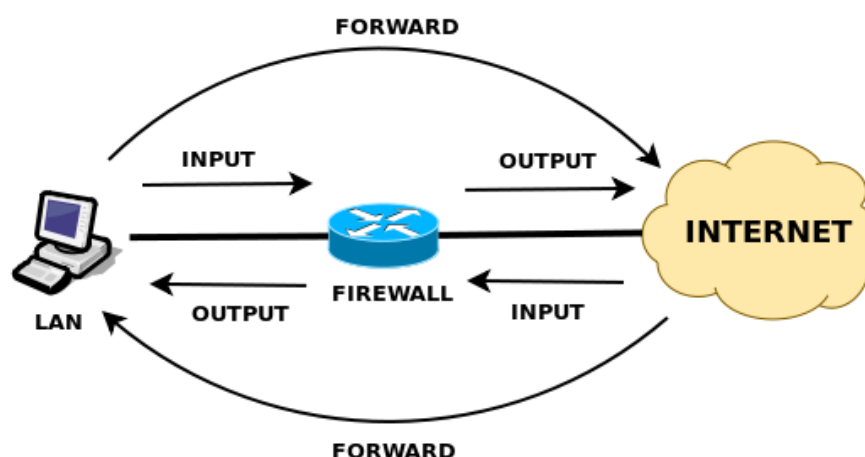
Firewall beroperasi berdasarkan rule firewall. Setiap rule berisi dua bagian, bagian yang mencocokkan arus lalu lintas jaringan dengan kondisi yang diberikan dan action yang mendefinisikan apa yang harus dilakukan dengan paket yang telah dicocokkan.

Rule filtering firewall dikelompokkan ke dalam suatu chain. Chain memperbolehkan

suatu paket untuk dicocokkan dengan satu kriteria pada satu chain dan diteruskan untuk pemrosesan dengan beberapa kriteria lain ke chain yang lainnya. Sebagai contoh sebuah paket harus dicocokkan terhadap pasangan IP address dan port. Tentu saja, hal ini dapat dicapai dengan menambahkan pasangan IP address dan port sebanyak yang dibutuhkan ke suatu chain forward, tetapi terdapat cara yang lebih baik adalah dengan menambahkan satu rule yang mencocokkan lalu lintas dari suatu IP tertentu, sebagai contoh `/ip firewall filter add src-address=1.1.1.2/32 jump-target="mychain"` dan jika hal ini tepat dengan salah satu IP address paket maka akan diteruskan ke chain yang lain. Maka rule yang melakukan pencocokan terhadap port yang berbeda dapat ditambahkan ke chain "mychain" tanpa harus menspesifikasikan IP address lagi.

Terdapat tiga chain bawaan dari table filter, yang tidak bisa dihapus:

- **Input**, digunakan untuk memproses paket yang masuk ke router melalui dari salah satu interface dengan IP address tujuan adalah salah satu dari alamat router. Paket yang melewati router tidak akan diproses pada rule di chain input.
- **Forward**, digunakan untuk memproses paket yang melewati router.
- **Output**, digunakan untuk memproses paket yang berasal dari router dan pergi meninggalkan router dari salah satu interface. Paket yang melewati router tidak akan diproses pada rule di chain output.



Gambar 11 Chain pada table Filter

Ketika sedang memproses suatu chain, rule-rule akan diambil dari chain dengan urutan

dimana mereka didaftarkan dari atas ke bawah. Jika suatu paket sesuai dengan salah satu kriteria rule, maka action yang telah dispesifikasikan akan dijalankan dan tidak ada rule yang akan diproses pada chain. Jika paket tidak sesuai dengan rule apa pun maka akan diterima.

Sebagai contoh Anda ingin mengamankan akses router dari internet. Akses ke router yang diperbolehkan aplikasi jaringan FTP, SSH, HTTP dan ping sedangkan akses jaringan yang lain tidak diperbolehkan. Asumsi interface router yang ke internet adalah ether1. Port jaringan yang dipakai adalah:

- FTP nomor port 20 dan 21
- SSH nomor port 22
- HTTP nomor port 80
- ping menggunakan protokol icmp

Maka konfigurasinya adalah:

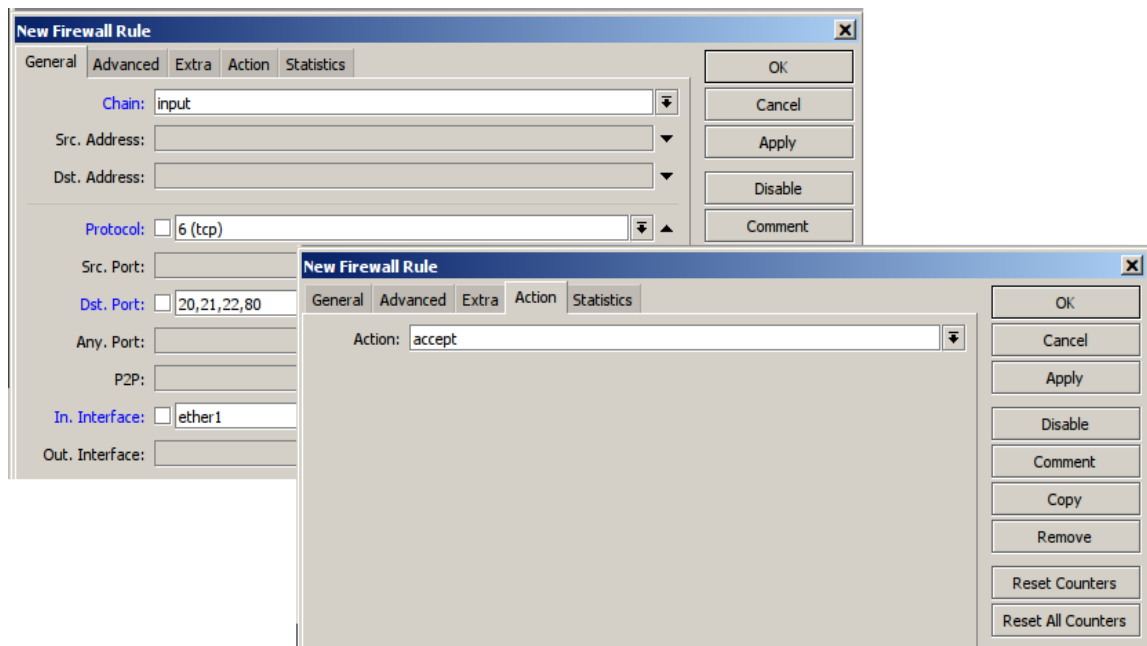
1. Klik IP → Firewall → pilih tab Filter. Kemudian klik tombol + untuk setiap konfigurasi filter yang dibuat.
2. Konfigurasi untuk menerima akses FTP, SSH dan HTTP

Pada tab General

- Chain: input
- Protocol: (6) tcp
- Dst Port: 20,21,22,80
- In Interface: ether1

Pada tab Action

- Action: accept



Gambar 12 Pemberian akses untuk FTP, SSH dan HTTP

3. Konfigurasi untuk menerima akses ICMP

Pada tab General

- Chain: input
- Protocol: (1) icmp
- In Interface: ether1

Pada tab Action

- Action: accept

4. Konfigurasi untuk menerima akses balik atas koneksi yang telah terjalin

Pada tab General

- Chain: input
- In Interface: ether1
- Connection state: established

5. Pada tab Action

- Action: accept

Kemudian tambahkan rule

Pada tab General

- Chain: input
- In Interface: ether1
- Connection state: related

6. Pada tab Action

- Action: accept

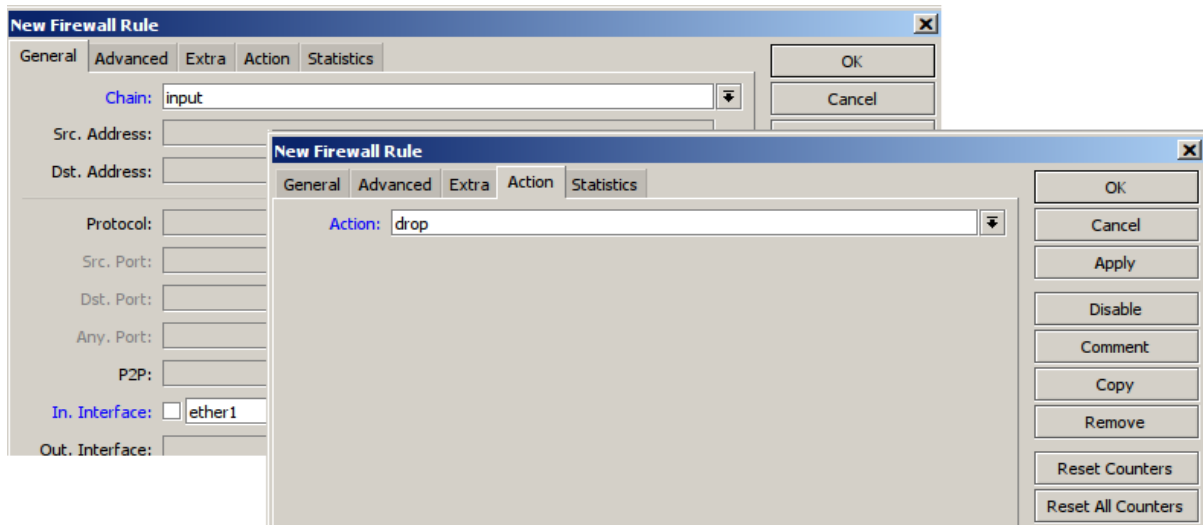
7. Konfigurasi untuk memblokir akses lainnya.

Pada tab General

- Chain: input
- In Interface: ether1

8. Pada tab Action

- 9. Action: drop



Gambar 13 Pemblokiran akses lain ke Server

Konfigurasi command linanya:

```
[admin@MikroTik] > /ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=20,21,22,80 action=accept
[admin@MikroTik] > /ip firewall filter add chain=input in-interface=ether1 protocol=icmp action=accept
[admin@MikroTik] > /ip firewall filter add chain=input in-interface=ether1 con action=accept
[admin@MikroTik] > /ip firewall filter add chain=input in-interface=ether1 connection-state=related action=accept
[admin@MikroTik] > /ip firewall filter add chain=input in-interface=ether1 connection-state=established action=accept
[admin@MikroTik] > /ip firewall filter add chain=input in-interface=ether1 action=drop
```

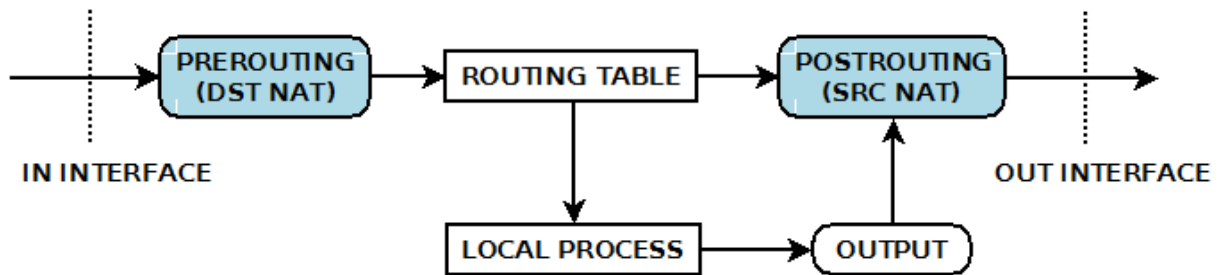
3.4 NAT

NAT atau Network Address Translation adalah standard internet yang memperbolehkan suatu host pada LAN untuk menggunakan satu set dari IP address untuk komunikasi internak dan set lainnya untuk IP address untuk komunikasi internal. Sebuah LAN yang menggunakan NAT disebut natted network. Supaya NAT dapat berfungsi, maka dibutuhkan NAT gateway untuk setiap natted network. NAT gateway (NAT router) menjalankan penulisan ulang IP address ketika paket melewati dari/ke suatu LAN.

Terdapat dua tipe dari NAT:

- **source NAT** atau **srcnat**. NAT tipe ini dijalankan pada suatu paket yang berasal dari natted network. Sebuah router NAT mengganti IP address privat dari suatu paket IP dengan IP address publik baru ketika berjalan melewati router. Operasi kebalikan dari NAT ini akan dijalankan untuk paket balasan yang berjalan ke arah sebaliknya. Source NAT melakukan penggantian paket IP yang keluar dari router maka Anda bisa mendefinisikan out interface Anda.
- **Destination NAT** atau **dstnat**, NAT tipe ini dijalankan pada suatu paket yang bertujuan ke natted network. Rule ini paling umum digunakan untuk membuat host pada jaringan privat supaya dapat diakses dari internet. Sebuah NAT melakukan dstnat mengganti IP address tujuan dari paket IP ketika berjalan melewati router ke jaringan privat. Destination NAT melakukan penggantian paket IP yang masuk ke router maka Anda bisa mendefinisikan in interface Anda.

Host dibelakang NAT router tidak memiliki koneksi end-to-end yang sebenarnya. Oleh karena itu beberapa protokol internet tidak dapat bekerja dengan skenario NAT. Service yang membutuhkan inisiasi dari koneksi TCP dari jaringan luar ke jaringan privat atau protokol stateless seperti UDP, dapat menjadi error. Terlebih lagi beberapa protokol tidak bisa menggunakan NAT, sebagai contoh protokol AH dari Ipsec.



Gambar 14 Letak Chain Tabel NAT pada Arus Paket Data di Router

3.4.1 Source NAT

Jika Anda hendak menyembunyikan IP privat di LAN 172.16.10.0/24 di belakang satu alamat 202.15.23.78 yang diberikan kepada Anda oleh ISP, Anda sebaiknya menggunakan fitur source NAT (masquerading) pada router Mikrotik. Masquerading akan mengganti source IP address dan port paket berasal dari 172.16.10.0/24 ke alamat 202.15.23.78 yang dimiliki router ketika paket tersebut dirouting melewatinya.

Untuk melakukan masquerading, sebuah rule source NAT dengan action masquerade harus ditambahkan pada konfigurasi firewall. Hal ini sesuai yang dibahas pada pengaturan sharing internet. Cara lain adalah dengan menggunakan action “src-nat” untuk melakukan pemetaan secara statis.

Untuk konfigurasinya:

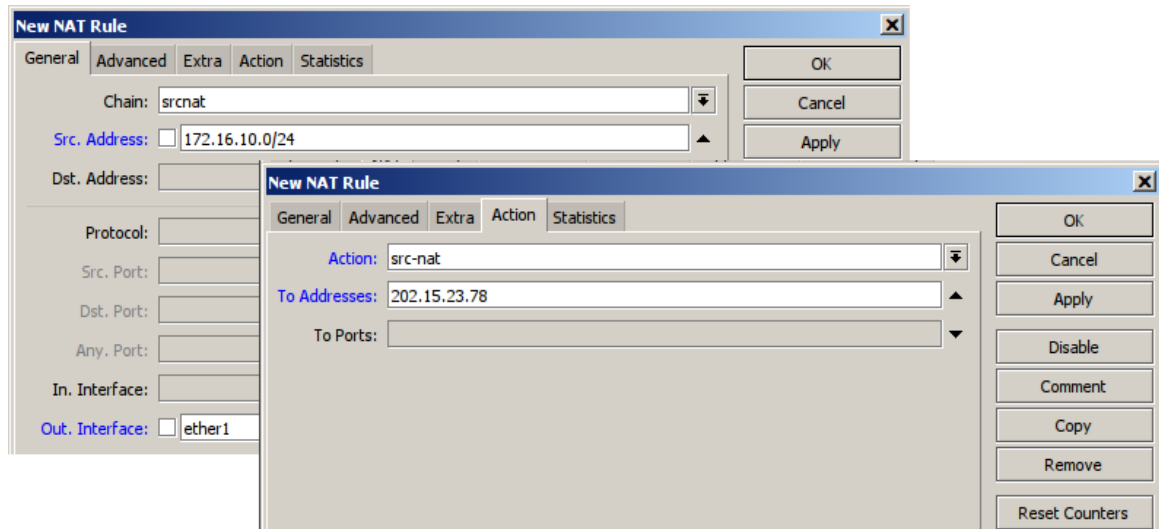
1. Klik IP → Firewall. Pilih tab NAT kemudian klik tombol +.
2. Masukkan konfigurasi berikut:

Pada tab General

- Chain: srcnat
- Out Interface: ether1
- Src Address: 172.16.10.0/24

3. Pada tab Action

- Action: src-nat
- To Addresses: 202.15.23.78



Gambar 15 Konfigurasi Source NAT

Konfigurasi command linanya:

```
[admin@MikroTik] > /ip firewall nat add chain=srcnat out-interface=ether1
src-address=172.16.10.0/24 action=src-nat to-addresses=202.15.23.78
```

3.4.2 Destination NAT

Jika Anda hendak untuk menghubungkan IP publik 202.15.23.78 ke IP privat 172.16.10.150, Anda harus menggunakan fitur destination NAT dari router Mikrotik. Jika Anda ingin memperbolehkan server di lokal untuk berkomunikasi dengan jaringan luar dengan publik IP yang diberikan maka Anda sebaiknya juga menggunakan source address translation. Untuk konfigurasi source NAT terdapat pada poin sebelumnya.

Untuk konfigurasinya adalah:

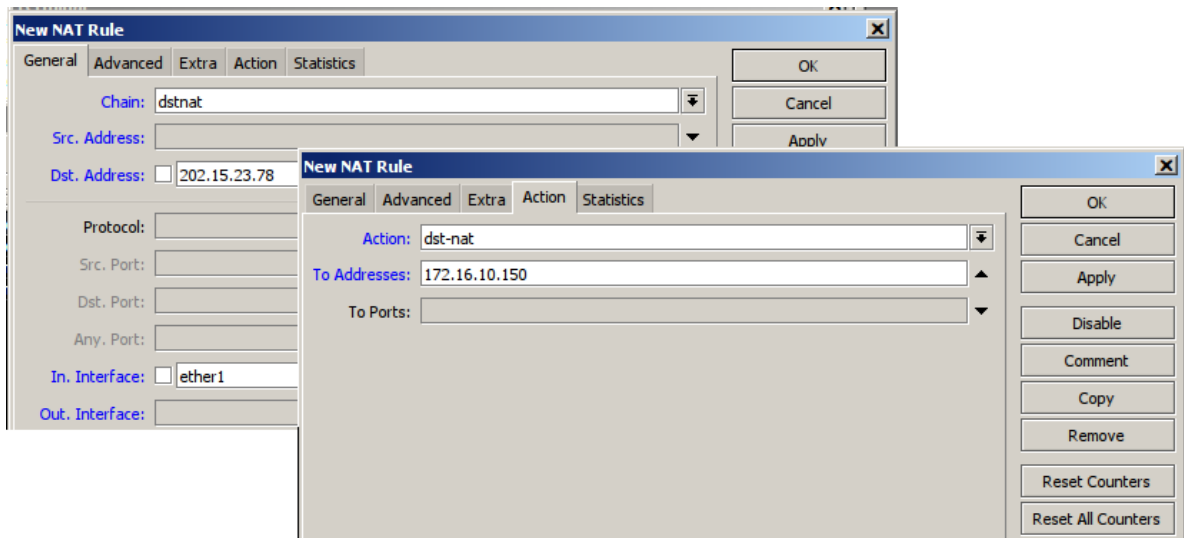
1. Klik IP → Firewall. Pilih tab NAT kemudian klik tombol +.
2. Masukkan konfigurasi berikut:

Pada tab General

- Chain: dstnat
- In Interface: ether1
- Dst Address: 202.15.23.78

Pada tab Action

- Action: dst-nat
- To Addresses: 172.16.10.150



Gambar 16 Konfigurasi Destination NAT

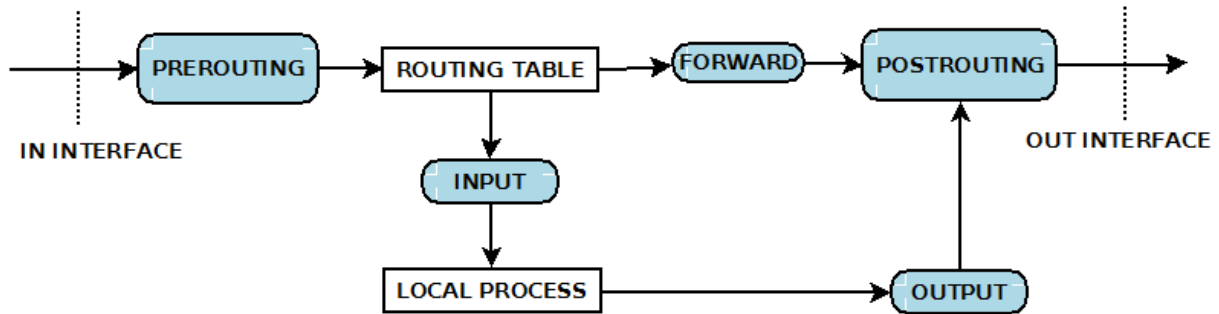
Konfigurasi command linanya:

```
[admin@MikroTik] > /ip firewall nat add chain=dstnat dst-address=10.5.8.200 in-interface= ether1 action=dst-nat to-addresses=192.168.0.109
```

3.5 Mangle

Table Mangle berfungsi untuk menandai paket untuk proses selanjutnya. dengan menggunakan tanda (mark) khusus. Beberapa fasilitas di RouterOS menggunakan tanda tersebut, seperti queue, NAT, routing, yang akan memproses paket berdasarkan tanda yang dimilikinya dan memproses sesuai dengan yang diinginkan. Tanda dari mangle hanya ada pada router, tanda tersebut tidak dikirimkan ke jaringan lain.

Fasilitas mangle juga dapat melakukan perubahan pada beberapa field pada IP header seperti TOS (DSCP) dan field TTL.



Gambar 17 Letak Chain Table Mangle pada Arus Paket Data di Router

Tipe-tipe mark pada tabel Mangle:

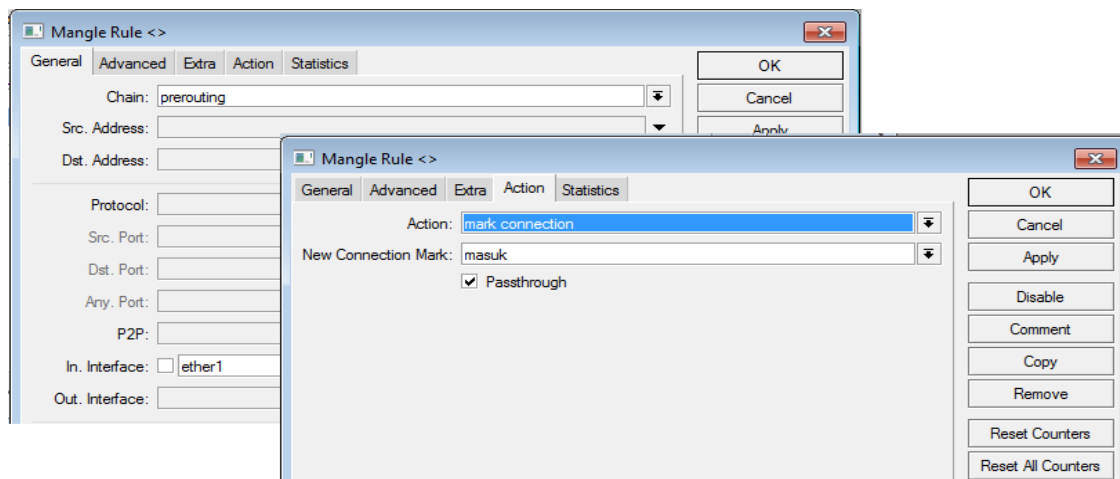
- Packet Mark
- Connection Mark
- Route Mark

Contoh 1:

Anda hendak menandai paket yang masuk dan keluar dari interface ether1. Untuk paket yang masuk ke ether1 maka berikan tanda pada chain prerouting dan untuk paket yang keluar maka berikan tanda pada chain postrouting.

Konfigurasi sebagai berikut:

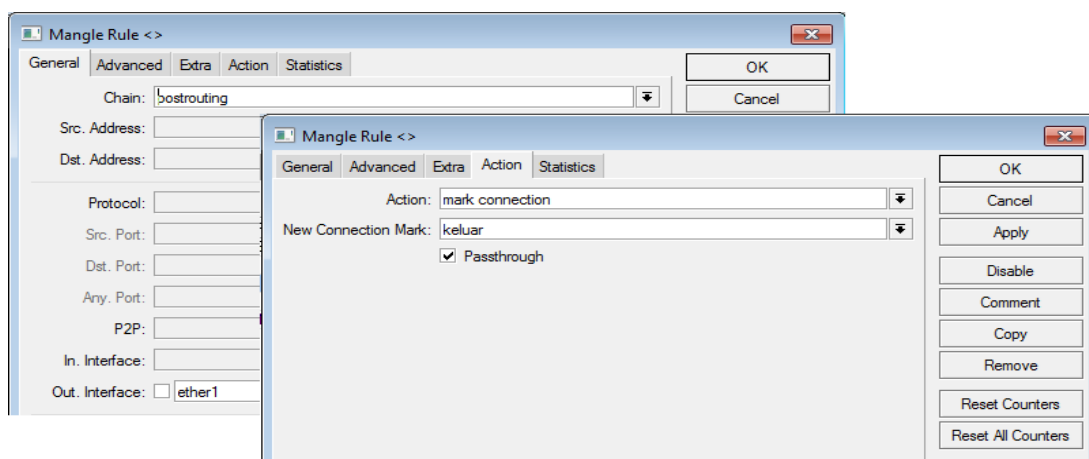
1. Klik IP → Firewall → klik tab Mangle. Untuk rule baru tekan tombol +.
2. Konfigurasi untuk menandai paket yang masuk ke ether1 sebagai berikut:
 - Chain: Prerouting
 - In Interface: ether1
 - Action: Mark Connection
 - New Connection Mark: masuk



Gambar 18 Konfigurasi Mangle Paket yang Masuk ke ether 1

3. Konfigurasi untuk menandai paket yang keluar dari ether1 sebagai berikut:

- Chain: Postrouting
- In Interface: ether1
- Action: Mark Connection
- New Connection Mark: keluar



Gambar 19 Konfigurasi Mangle Paket yang Keluar dari ether1

Konfigurasi Command Line:

```
[admin@MikroTik] > /ip firewall mangle add chain=prerouting in-interface=ether1
action=mark-connection new-connection-mark=masuk
```

```
[admin@MikroTik] > /ip firewall mangle add chain=postrouting out-interface=ether1
action=mark-connection new-connection-mark=keluar
```

BAB 4

VPN

Tujuan:

- Mahasantri mengetahui tentang teknologi VPN
- Mahasantri mengetahui cara membuat PPTP server pada router
- Mahasantri mengetahui cara mengkonfigurasi PPTP client pada router

4.1 VPN

VPN (Virtual Private Network) adalah suatu jaringan yang menggunakan infrastruktur telekomunikasi publik, seperti Internet untuk menyediakan remote ke kantor atau akses ke jaringan pusat untuk user yang sedang bepergian.

VPN pada umumnya membutuhkan remote user dari suatu jaringan untuk melakukan autentikasi dan melakukan pengamanan data dengan teknologi enkripsi untuk mencegah pengaksesan dari user-user yang tidak berhak terhadap data-data rahasia atau pribadi.

Komputer pada jaringan VPN dapat melakukan semua fungsionalitas pada jaringan , seperti sharing data dan mengakses sumber daya jaringan, printer, database, website, dll. Sebuah user VPN pada umumnya ketika melakukan koneksi ke jaringan utama, seakan-akan terkoneksi langsung ke jaringan tersebut. Teknologi VPN melalui akses internet telah menggantikan kebutuhan untuk berlangganan koneksi komunikasi leased-line dedicated yang pernah digunakan pada instalasi WAN.

Router Mikrotik mendukung fitur VPN:

- PPTP
- EoIP
- L2TP
- MPLS
- IPSec

- VLAN

Dalam tulisan ini hanya akan dibahas PPTP dan EoIP.

4.2 PPTP

PPTP adalah protokol tunnel yang aman digunakan untuk transportasi lalu lintas IP menggunakan PPP. PPP dienkapsulasikan PPTP pada jalur virtual yang berjalan melalui koneksi berbasis IP. PPTP memadukan PPP dan MPE (Microsoft Point to Point Encryption) untuk membuat link yang terenkripsi. Tujuan dari protokol ini adalah untuk membuat koneksi yang aman dan dikelola dengan baik antara router dan juga antara router dengan klien PPTP.

Multilink PPP (MP) didukung untuk menyediakan MRRU (kemampuan untuk mentransmisi paket secara penuh 15000 byte atau lebih) dan melakukan bridging melalui link PPP (menggunakan Bridge Control Protocol – BCP, yang memperbolehkan untuk mengirim raw frame Ethernet melalui link PPP). Dengan cara ini maka Anda bisa mengkonfigurasi bridge tanpa EoIP. Bridge harus memiliki pengaturan MAC address atau interface seperti Ethernet, sedangkan link PPP tidak memiliki MAC Address.

PPTP memasukan autentikasi dan akunting dari PPP untuk setiap koneksi PPTP. Autentikasi dan akunting penuh dari setiap koneksi bisa dilakukan melalui klien RADIUS atau secara lokal. Enkripsi MPPE 40bit RC4 dan MPPE 128bit RC4 didukung.

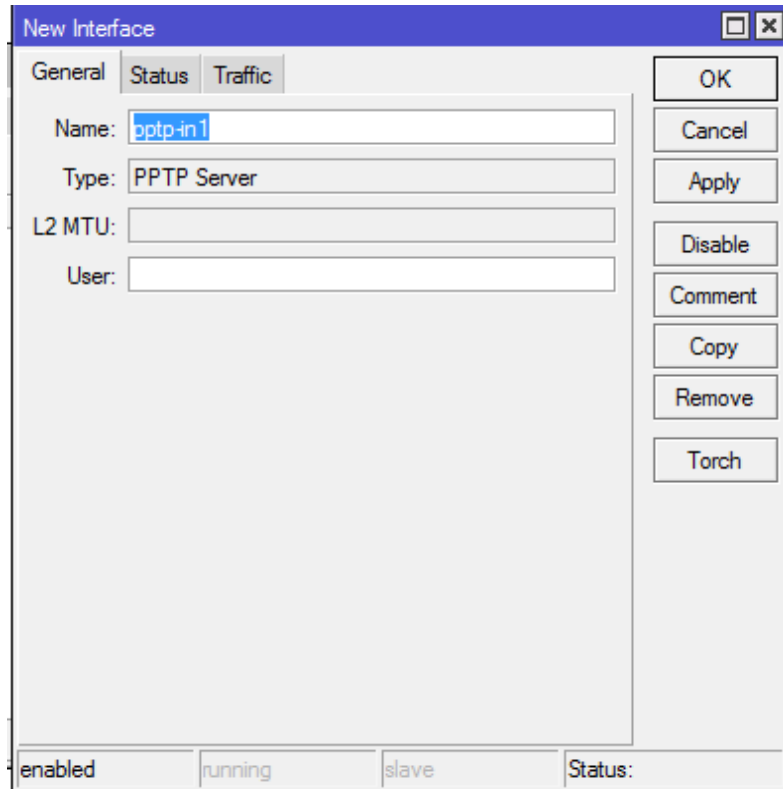
PPTP menggunakan TCP port 1723 dan protokol IP GRE (Generic Routing Encapsulation, protokol IP ID 47), seperti yang diberikan dari Internet Assigned Number Authority (IANA). PPTP dapat digunakan dengan sebagian besar firewall dan router dengan mengaktifkan lalu lintas yang menuju port 1723 dan ke protokol 47 untuk dirouting melewati firewall atau router.

Koneksi PPTP memiliki keterbatasan atau mustahil di konfigurasi melalui masquerade atau koneksi IP NAT.

4.2.1 Konfigurasi PPTP Server

1. Mengaktifkan Interface PPTP Server

1. Klik PPP → Klik tombol + → pilih PPTP Server.
2. Masukkan Nama dari PPTP Server

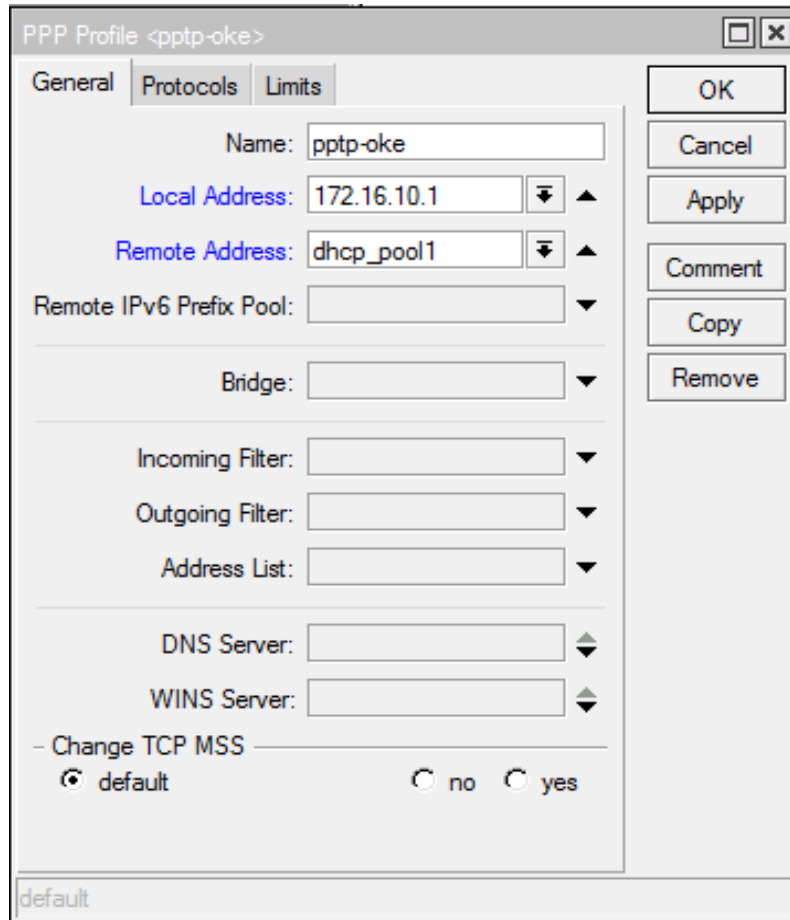


Gambar 20 Mengaktifkan server PPTP

3. Buat profile PPTP, klik PPP → pilih tab Profile → Klik tombol +
Masukkan sebagai berikut:

- Name, diisi dengan nama PPTP Profile
- Local Address, diisi dengan IP address yang akan dimiliki oleh interface PPTP Anda.
- Remote Address diisi dengan jangkauan alamat yang akan diberikan ke client. Dalam hal ini IP address dari 172.16.10.2 sampai 172.16.10.254. Dikonfigurasi dengan perintah:

```
[admin@MikroTik] > /ip pool add name=dhcp_pool1 ranges=172.16.10.2-172.16.10.254
```



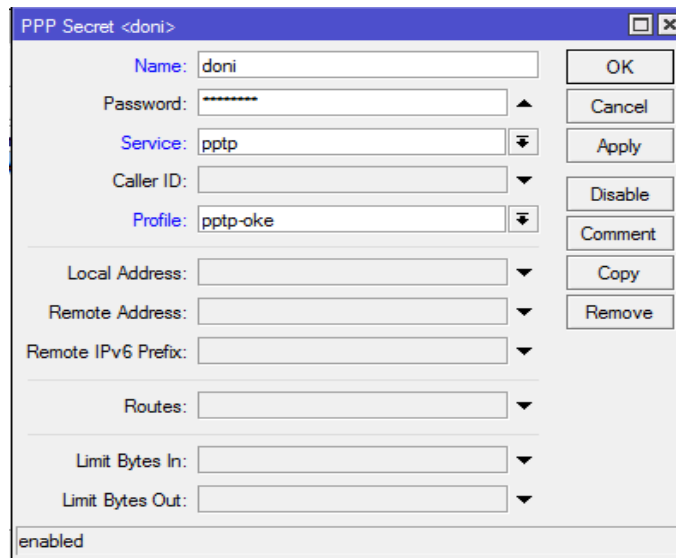
The screenshot shows the 'PPP Profile <pptp-oke>' configuration window in Mikrotik WinBox. The 'General' tab is selected. The configuration includes:

- Name: pptp-oke
- Local Address: 172.16.10.1
- Remote Address: dhcp_pool1
- Remote IPv6 Prefix Pool: (empty)
- Bridge: (empty)
- Incoming Filter: (empty)
- Outgoing Filter: (empty)
- Address List: (empty)
- DNS Server: (empty)
- WINS Server: (empty)
- Change TCP MSS: ☒ default, ☐ no, ☐ yes

Buttons on the right: OK, Cancel, Apply, Comment, Copy, Remove. A 'default' button is at the bottom left.

Gambar 21 Pembuatan file PPTP

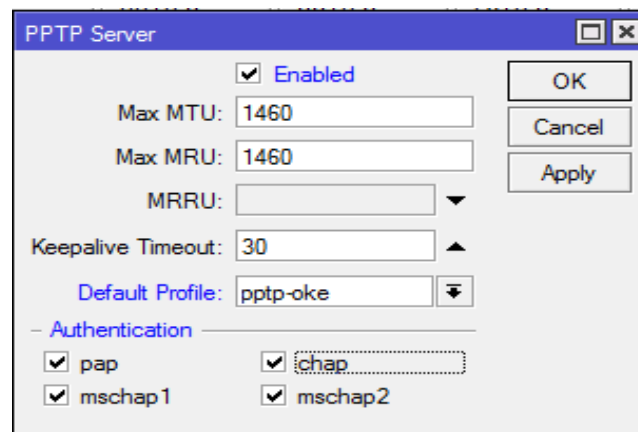
4. Kemudian Anda harus membuat akun untuk autentikasi ke PPTP sesuai dengan PPTP profile. Masukkan pada:
 - Name, diisi dengan nama user yang digunakan
 - Password, diisi dengan password dari user
 - Service, untuk pemilihan protokol yang diperbolehkan menggunakan akun ini.
 - Profile, pemilihan profile yang diperbolehkan menggunakan akun ini.



Gambar 22 Pembuatan security PPTP

5. Kemudian Anda aktifkan PPTP server Anda dengan mengklik PPP → pada tab Interface klik PPTP Server. Konfigurasi pada:

1. Centang pada bagian Enabled
2. Default Profile, isikan dengan profile PPTP yang hendak digunakan.
3. Authentication Anda diminta metode autentikasi yang Anda gunakan:
 - PAP (Password Authentication Protocol), menggunakan autentikasi dengan mengirimkan password ASCII yang tidak terenkripsi, maka dianggap kurang aman.
 - CHAP (Challenge-Handshake Authentication Protocol), merupakan autentikasi dengan cara secara periodik memverifikasi identitas dari client dengan menggunakan three-way handshake. Pada CHAP autentikasi dilakukan secara terenkripsi sehingga lebih aman.
 - MS-CHAP1 & 2, adalah versi Microsoft dari CHAP.



Gambar 23 Pemilihan Profile

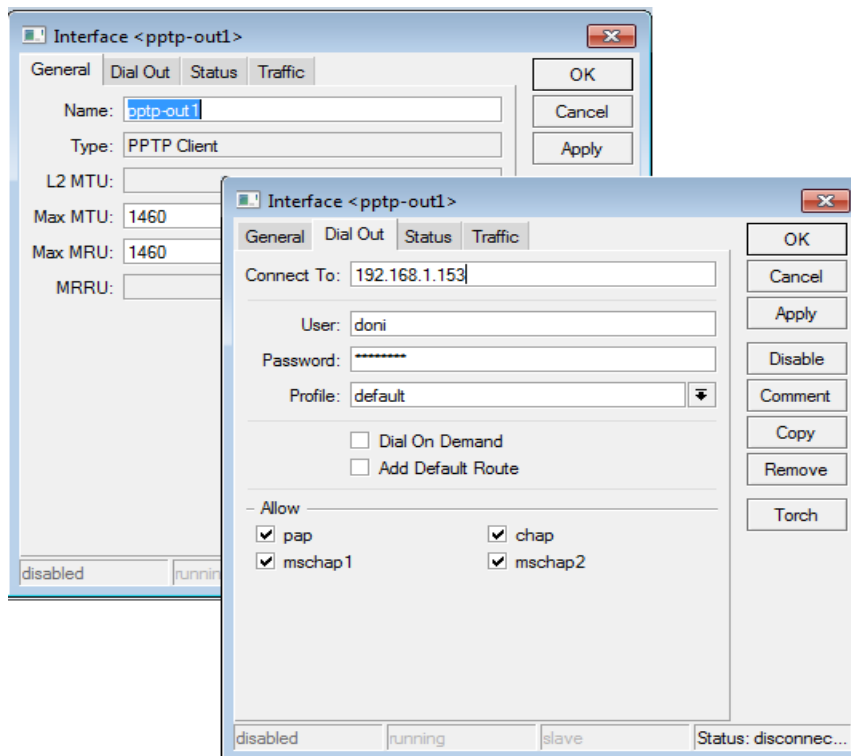
4.2.2 Konfigurasi PPTP Client

Anda bisa mengatur RouterOS Anda sebagai PPTP Client dengan cara sbb:

1. Klik PPP → Pada tab Interface klik Tombol + → pilih PPTP Client
2. Pada Tab General isikan:
 - Name : Masukkan nama interface PPTP client Anda

Kemudian klik Dial Out:

- Connect to, isikan dengan IP address atau hostname dari PPTP server.
 - User, masukkan username dari PPTP Server Anda.
 - Password, masukkan password dari username di atas
3. Bila sudah klik OK



Gambar 24 Konfigurasi PPTP Client

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /interface pptp-client add name=pptp-out connect
to=192.168.1.153 user=doni password=password
```

4.3 EoIP

Ethernet over IP (EoIP) adalah protokol dari Mikrotik RouterOS yang membuat tunnel Ethernet antara dua router di atas koneksi IP. Tunnel EoIP dapat berjalan di atas tunnel IPIP, tunnel PPTP atau koneksi lain yang mampu mentransport IP. Ketika fungsi bridge dari router diaktifkan, semua lalu lintas ethernet (semua protokol ethernet) akan di bridge seakan-akan terdapat sebuah interface ethernet fisik dan kabel diantara kedua router (dengan bridge aktif). Protokol ini membuat beberapa skema jaringan dapat dilakukan.

Beberapa kemungkinan konfigurasi jaringan untuk interface EoIP:

- Dapat membuat bridge LAN melalui internet

- Dapat membuat bridge LAN melalui tunnel yang dienkripsi
- Dapat membuat bridge LAN melalui jaringan wireless 'ad-hoc' 802.11b

Protocol EoIP mengenkapsulasi frame ethernet pada paket GRE (seperti pada PPTP) dan mengirimkan mereka ke ujung dari tunnel EoIP.

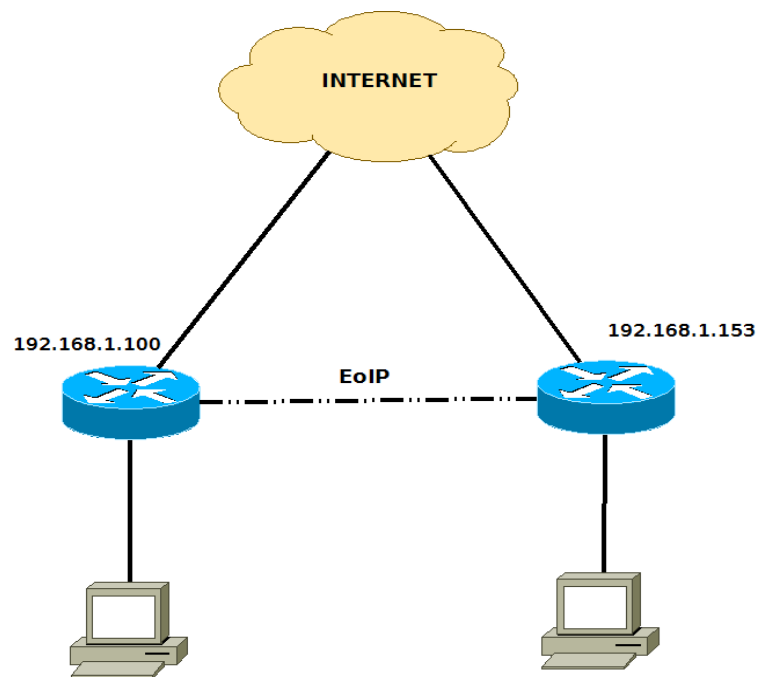
Sebuah interface EoIP harus dikonfigurasi dengan dua router yang memiliki kemampuan untuk koneksi di tingkat IP. Tunnel EoIP dapat berjalan pada tunnel IPIP, tunnel PPTP dengan enkripsi 128 bit, koneksi PPPoE, atau koneksi apa pun yang menggunakan IP.

Beberapa spesifikasi dari EoIP:

- Setiap interface tunnel EoIP dapat terhubung dengan satu remote router, yang menggunakan interface yang serupa dengan konfigurasi 'Tunnel ID' yang sama.
- Interface EoIP tampil sebagai interface ethernet pada daftar interface
- Interface ini mendukung semua fitur dari interface ethernet. IP address dan tunnel yang lainnya dapat dijalankan di atas interface.
- Protokol EoIP mengenkapsulasi frame ethernet pada paket GRE (seperti pada PPTP) dan mengirimkan mereka ke ujung dari tunnel EoIP.
- Jumlah maksimal dari tunnel EoIP adalah 65536
- Maximal count of EoIP tunnels is 65536.

4.3.1 Konfigurasi EoIP

Misalkan Anda hendak menghubungkan dua RouterOS dengan menggunakan EoIP dengan bentuk jaringan sebagai berikut:

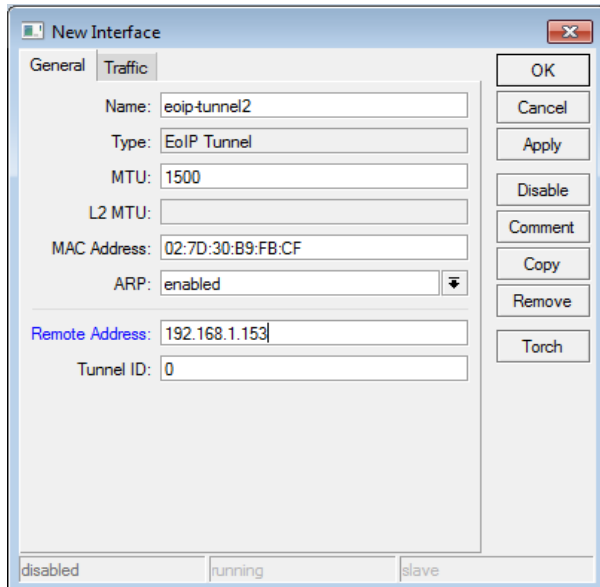


Gambar 25 Contoh Jaringan dengan EoIP

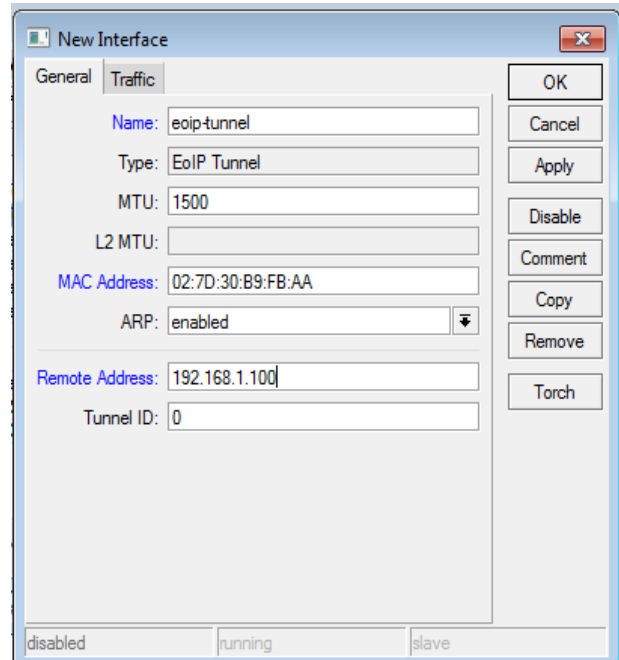
Konfigurasinya sebagai berikut:

1. Pada kedua router, Klik Interface → klik tombol + → Pilih EoIP Tunnel.
2. Konfigurasikan sebagai berikut:
 - Name, masukkan nama interface EoIP
 - Remote Address, masukkan IP address dari router yang menjadi ujung dari tunnel EoIP yang Anda buat.
 - MAC Address, berisi MAC Address dari interface, bila sama dengan interface EoIP di router yang dihubungkan dengan router ini, maka harus diubah.

- Tunnel ID, diisi dengan ID dari tunnel EoIP yang digunakan. Kedua router yang dihubungkan harus memiliki Tunnel ID yang sama.



Gambar 26 Konfigurasi EoIP Router di Kiri



Gambar 27 Konfigurasi EoIP Router di Kanan

3. Bila sudah dibuat interfacenya masukkan device EoIP ke dalam interface bridge Anda sehingga kedua LAN dapat saling berkomunikasi seakan-akan di dalam jaringan yang sama.

Konfigurasi Command Linenya:

- Router Kiri:

```
[admin@MikroTik] > /interface eoip add name=eoip-tunnel2 mac-address=02:70:30:B9:FB:CF remote-address=192.168.1.153 tunnel-id=0
```

- Router Kanan:

```
[admin@MikroTik] > /interface eoip add name=eoip-tunnel mac-address=02:70:30:B9:FB:AA remote-address=192.168.1.100 tunnel-id=0
```

BAB 5

HotSpot

Tujuan:

- Mahasantri dapat membatasi akses internet di jaringan dengan fitur Hotspot
- Mahasantri dapat melewati beberapa situs pada Hotspot
- Mahasantri dapat memperbolehkan beberapa klien pada Hotspot

5.1 HotSpot

Autentikasi pada wireless memiliki banyak kelemahan sehingga dibutuhkan metode untuk mengamankan jaringan wireless Anda. Salah satu caranya adalah dengan menggunakan fasilitas Hotspot pada RouterOS. Dengan menggunakan fitur ini maka Anda dapat mengotorisasi komputer mana saja yang dibolehkan untuk mengakses internet menggunakan jaringan Anda. Hotspot akan menyediakan autentikasi untuk klien sebelum mengakses jaringan publik.

Fitur Gateway Hotspot:

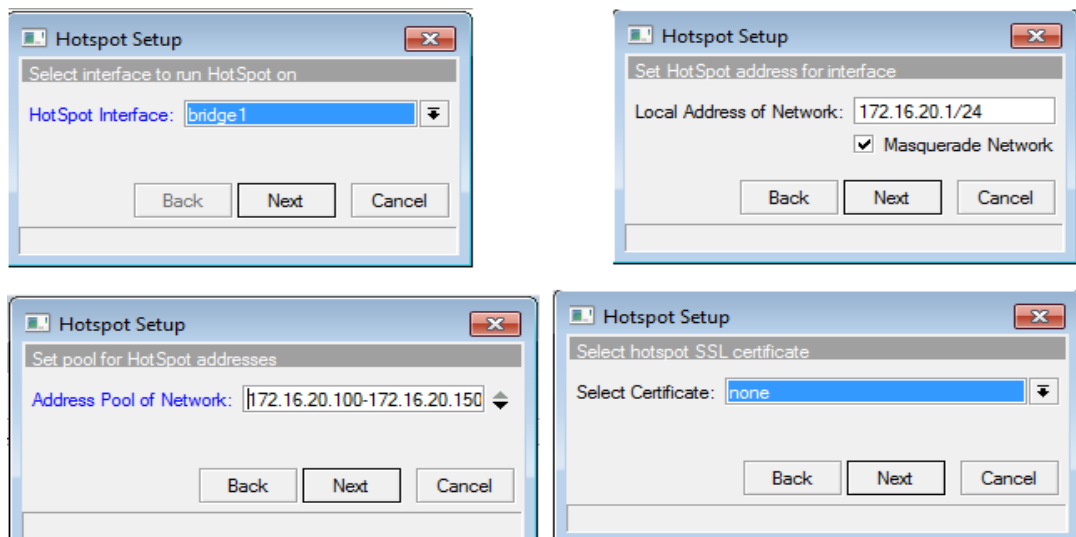
- Metode autentikasi yang berbeda untuk klien menggunakan database lokal di router atau menggunakan server RADIUS.
- Accounting user di database lokal atau di server RADIUS
- sistem walled garden, mengakses ke beberapa halaman web tanpa otorisasi.
- Modifikasi halaman login, dimana Anda dapat memasukkan informasi perusahaan Anda.
- Perubahan yang otomatis dan transparan IP address apapun dari suatu klien ke suatu alamat yang valid.

5.2 Konfigurasi HotSpot

1. Klik IP → Hotspot → Klik tombol Hotspot Setup

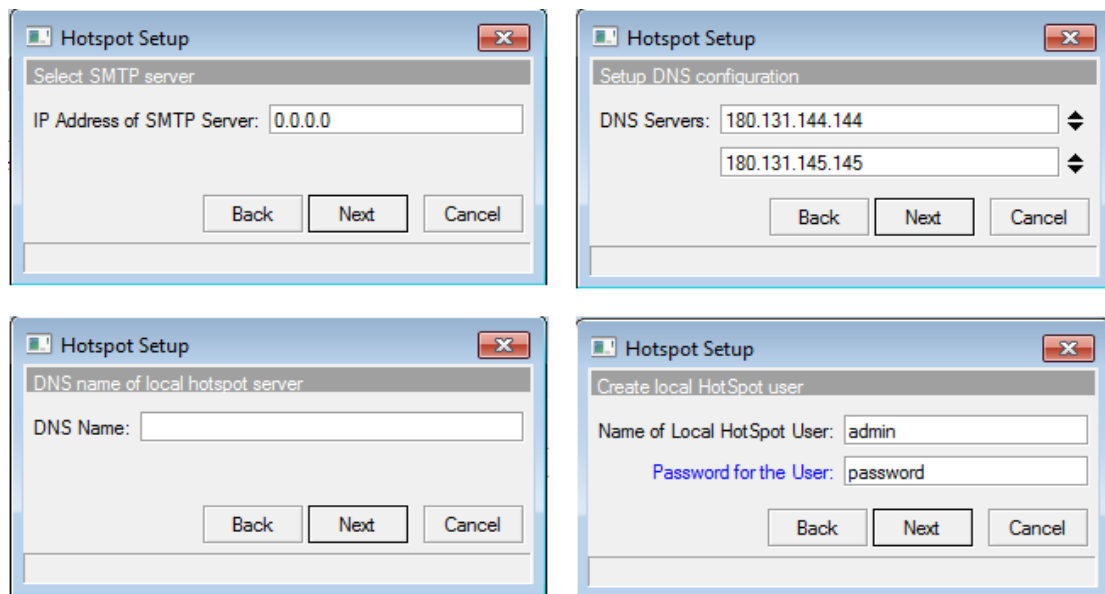
2. Kemudian ikuti langkah berikut:

- Hotspot Interface, masukkan interface yang akan diaktifkan fasilitas hotspot. Interface yang digunakan adalah interface yang terhubung ke jaringan LAN.
- Local Address of Network, diisikan dengan IP address dari IP dari router yang digunakan sebagai hotspot gateway.
- Address Pool of Network, diisikan dengan jangkauan IP address yang akan diberikan kepada klien hotspot.
- Select Certificate, digunakan apabila hotspot menggunakan otorisasi HTTPS, diisi dengan sertifikat SSL.



Gambar 28 Konfigurasi HotSpot Setup 1

- IP address of the SMTP server, IP address tujuan dimana permintaan SMTP (port 25) akan dialihkan pada jaringan Hotspot. Bila tidak dialihkan maka isikan dengan 0.0.0.0.
- DNS Server, diisikan dengan IP DNS Server untuk klien hotspot.
- DNS Name, nama domain dari server Hotspot.
- Name of Local Hotspot User, diisikan dengan nama pengguna dari Hotspot dan pada Password for User., diisikan dengan password dari pengguna.



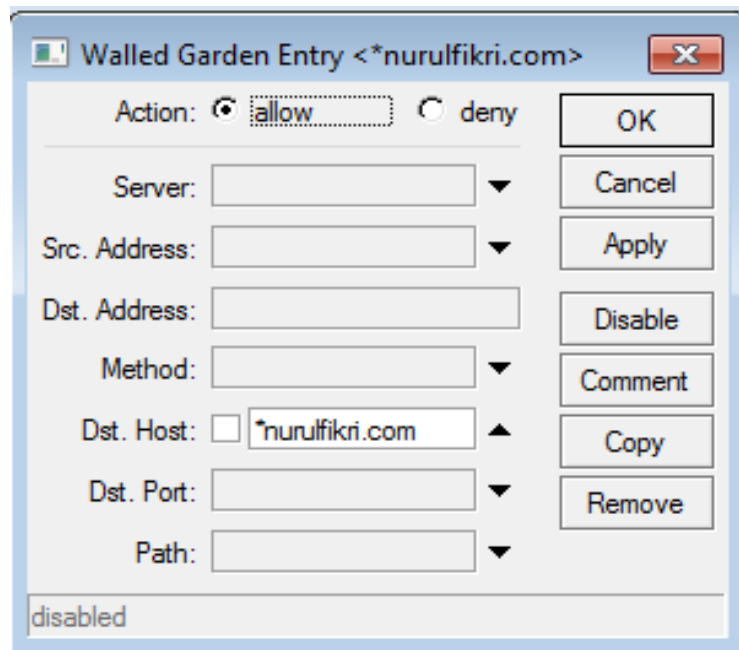
Gambar 29 Konfigurasi Setup Hotspot 2

5.3 Walled-Garden

HTTP Walled-Garden, digunakan untuk mengatur agar beberapa situs yang diminta melalui protokol HTTP atau HTTPS diteruskan tanpa perlu melakukan autentikasi.

Dalam hal ini akan dilewatkan akses ke nurulfikri.com tanpa perlu autentikasi di captive portal hotspot. Langkah konfigurasinya

1. Klik IP → Hotspot → Klik tab Walled-Garden → Klik tombol +.
2. Konfigurasi sbb:
 - Action: allow, berarti memperbolehkan akses ke situs.
 - Dst host: *nurulfikri.com. Isikan dengan situs tujuan yang akan diakses. Dalam hal ini adalah situs yang diperbolehkan di akses.



Gambar 30 Konfigurasi Walled Garden

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /ip hotspot walled-garden add action=allow dst-host=*nurulfikri.com
```

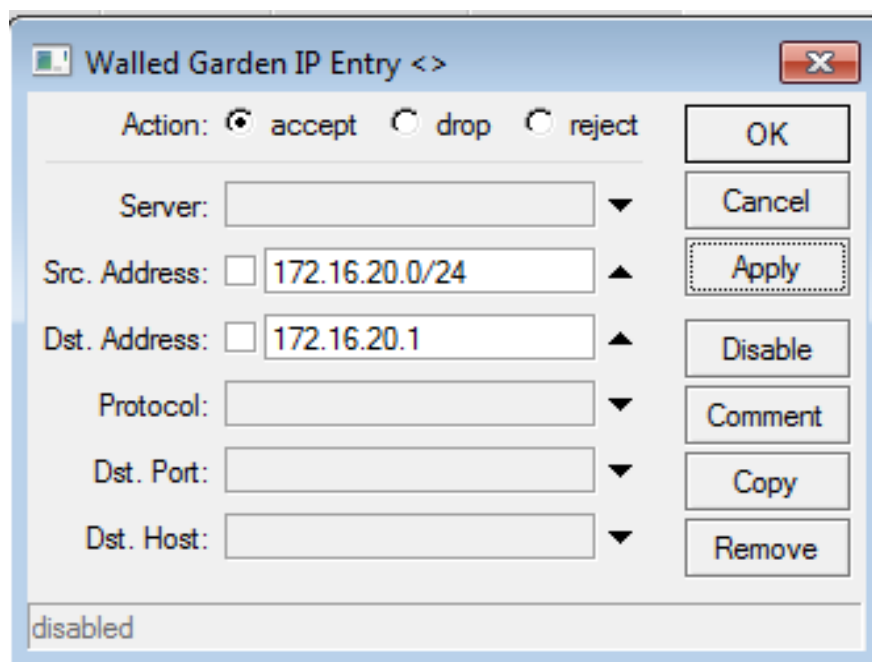
5.4 IP Walled-Garden

IP Walled Garden digunakan untuk memperbolehkan akses ke aplikasi jaringan yang lain selain HTTP ke jaringan luar. Pada jaringan hotspot apabila Anda belum diotentikasi maka Anda belum bisa terkoneksi ke jaringan luar maupun ke router menggunakan aplikasi jaringan apa pun. Dengan cara ini maka Anda dapat memperbolehkan aplikasi jaringan tertentu.

Sebagai contoh Anda hendak memberikan akses ke router pada komputer-komputer di jaringan hotspot. Nomor jaringan hotspot tersebut adalah 172.16.20.0/24. IP address router Anda 172.16.20.1. Maka langkah-langkahnya adalah:

- Klik IP → Hotspot → Klik tab Walled-Garden → Klik tombol +.
- Konfigurasi sbb:

1. Action: allow, Action digunakan untuk memberikan ijin untuk pengaksesan dari atau ke IP tertentu.
2. Src Address: 172.16.20.0/24, digunakan untuk menentukan alamat komputer klien yang meminta koneksi ke jaringan.
3. Dst Address: 172.16.20.1, digunakan untuk menentukan alamat tujuan yang hendak diakses oleh klien.



Gambar 31 Konfigurasi IP Walled-Garden

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /ip hotspot walled-garden ip add action=accept src-address=172.16.20.180 dst-host=172.16.20.1
```

BAB 6

QoS

Tujuan:

- Mahasantri mengetahui prinsip dari QoS
- Mahasantri dapat membatasi bandwidth dengan menggunakan simple queue

6.1 QoS

QoS (Quality of Service) adalah fasilitas dari komputer untuk menyediakan prioritas yang berbeda untuk aplikasi, user atau arus data atau untuk menjamin batas performa tertentu untuk suatu arus data. QoS umum digunakan pada jaringan dengan kapasitas yang terbatas, terutama untuk jaringan yang banyak menggunakan aplikasi streaming multimedia seperti VoIP, game online dan IP-TV. Hal ini dikarenakan dibutuhkan bit-rate yang tetap dan rentan terhadap delay,

Untuk melakukan pembatasan arus lalu lintas pada RouterOS QoS dilakukan dengan menggunakan fitur queue.

Queues digunakan untuk membatasi dan memprioritaskan lalu lintas jaringan :

- membatasi kecepatan transfer data untuk beberapa IP address, subnet, protokol, port dan parameter lain.
- Membatasi lalu lintas peer-to-peer.
- Memprioritaskan beberapa arus paket dibandingkan yang lain.
- Mengkonfigurasi burst traffic untuk browsing web yang lebih cepat.
- Mengaplikasikan batas yang berbeda berdasarkan waktu.
- Berbagi traffic yang ada antara beberapa user secara merata, atau berdasarkan jumlah permintaan dari channel.

Implementasi queue di Mikrotik RouterOS adalah berdasarkan Hierarchical Token Bucket (HTB). HTB memperbolehkan untuk membuat struktur hirarki queue dan menentukan relasi antar queue.

Pada RouterOS. Struktur hirarki ini dapat diberikan pada 4 tempat yang berbeda:

- global-in: merepresentasikan semua interface input pada umumnya (queue INGRESS). Queue yang dipasang pada global-in berlaku bagi semua lalu lintas jaringan yang diterima oleh router sebelum packet filtering.
- global-out: merepresentasikan semua interface output pada umumnya (queue EGRESS).
- global-total: merepresentasikan semua interface input dan output (dengan kata lain merupakan gabungan dari global-in dan global-out). Digunakan ketika pelanggan hanya memiliki satu pembatasan untuk keduanya, upload dan download.
- <interface name>: merepresentasikan satu interface keluar tertentu. Hanya lalu lintas jaringan yang diatur untuk keluar melalui interface ini akan melewati queue HTB.

Terdapat dua cara untuk melakukan konfigurasi queue pada RouterOS:

- /queue simple, didesain untuk memudahkan konfigurasi pengaturan queue yang sederhana. Seperti pembatasan upload/download suatu klien, pembatasan lalu lintas p2p, dll.
- /queue tree, untuk implementasi pekerjaan queue yang lebih kompleks, seperti pengaturan policy global, limitasi grup pengguna. Memerlukan penandaan arus paket dari fasilitas mangle pada firewall.

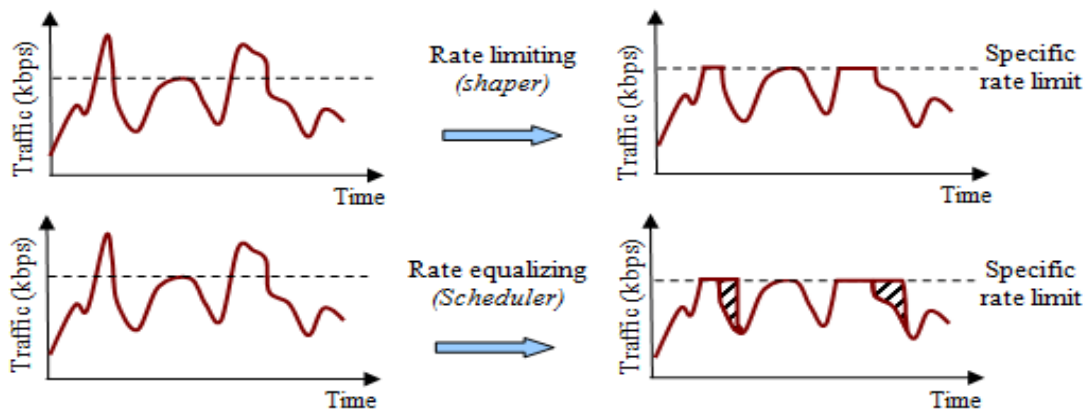
6.2 Prinsip Pembatasan Kecepatan

Pembatasan kecepatan digunakan untuk mengontrol kecepatan dari arus lalu lintas jaringan yang dikirim atau diterima oleh suatu perangkat jaringan. Lalu lintas yang kecepatannya kurang atau sama dengan yang ditentukan akan dikirim, sedangkan lalu lintas yang melebihi kecepatan yang ditentukan akan di drop atau ditunda.

Pembatasan kecepatan dapat dilakukan dengan dua cara:

1. Membuang semua paket yang melebihi batas kecepatan – rate limiting (dropper atau shapper)
2. Menunda paket yang melebihi batas kecepatan dan dikiri ketika keadaan memungkinkan – rate equalizing (scheduler).

Berikut perbedaan dari rate limiting dan equalizing



Gambar 32 Prinsip dari Rate Limiting dan Rate Equalizing

Seperti Anda lihat pada kasus pertama semua lalu lintas jaringan yang melebihi rate akan di-drop. Pada kasus kedua semua lalu lintas jaringan yang melebihi rate akan ditunda pada queue dan ditransmisikan nanti ketika memungkinkan., tetapi perlu diketahui bahwa paket dapat di ditunda hanya ketika queue tidak penuh. Jika tidak ada tempat lagi pada buffer queue, paket akan didrop.

Untuk setiap queue dapat kita definisikan dua batas rate:

- CIR (Committed Information Rate) – (limit-at pada RouterOS) pada skenario paling buruk, arus akan mendapatkan sesuai dengan rate yang diberikan tidak peduli arus jaringan yang lain. Setiap saat, bandwidth tidak akan turun dibawah dari CIR.
- MIR (Maximum Information Rate) – (max-limit pada RouterOS) adalah maximum rate data lalu lintas jaringan, terjadi apabila terdapat ada bagian bandwidth yang belum terpakai.

6.3 Simple Queues

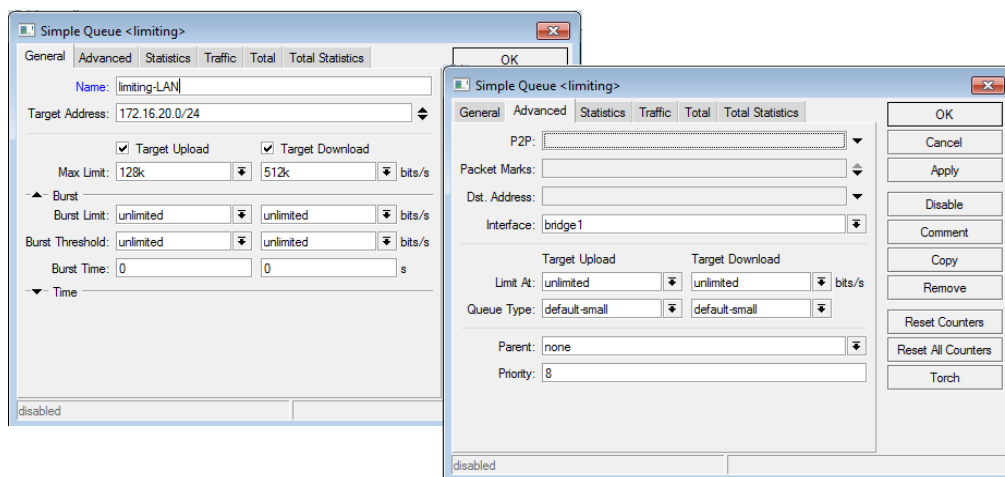
Cara paling mudah untuk membatasi rate data untuk IP address tertentu atau sebuah subnet, adalah dengan menggunakan simple queue. Anda juga bisa menggunakan simple queue untuk aplikasi QoS tingkat lanjut. Simple queue memiliki fitur yang terintegrasi:

- Queuing lalu lintas jaringan peer-to-peer

- Mengaplikasikan aturan queue pada interval waktu tertentu
- Prioritas
- Menggunakan mangle di firewall untuk penandaan beberapa paket.
- Shaping dari lalu lintas dua arah (satu limit untuk total dari upload + download)

Misalkan Anda hendak membatasi jaringan Anda agar hanya memiliki kecepatan 128kbps untuk upload dan download 512 kbps. Dalam contoh digunakan jaringan 172.16.20.0/24. Maka langkah konfigurasinya:

1. Klik Queues → Pilih tab Simple Queues → Klik tombol +.
2. Masukkan konfigurasi berikut:
3. Pada tab General, centang pada Target Upload dan Target Download untuk membatasi kecepatan download dan upload:
 - Name, adalah nama dari Queue
 - Target Address, adalah alamat tujuan yang akan dikenakan queue
 - Max Limit, masukkan kecepatan maksimal yang bisa dimiliki oleh keseluruhan jaringan.



Gambar 33 Konfigurasi Simple Queue

4. Pada tab Advanced
 - Interface, adalah interface yang terhubung dengan jaringan yang dibatas

Bab 7

Routing

Tujuan:

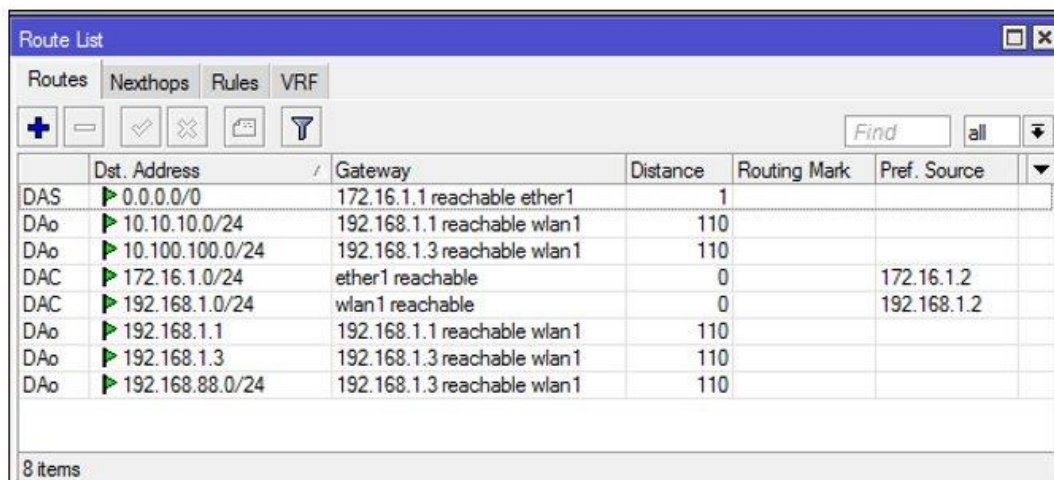
- Mahasantri mengetahui konsep dan prinsip dari routing
- Mahasantri dapat mengetahui teknik routing static
- Mahasantri dapat mengetahui teknik routing dynamic

7.1 Konsep Routing

Routing adalah proses penentuan jalur terbaik (*best path*) untuk mencapai suatu network tujuan. Routing juga dapat berarti proses memindahkan paket data dari host pengirim ke host tujuan dimana host pengirim dan host tujuan tidak berada dalam satu jaringan (network).

Pada saat melakukan routing, router akan menyimpan berbagai informasi routing sehingga dapat menentukan kemana sebuah paket atau traffic akan dikirimkan. Informasi routing ini berisi jalur terbaik (*best path*) yang sebaiknya ditempuh oleh sebuah paket.

Informasi routing disimpan oleh router pada sebuah tabel yang disebut tabel yang disebut tabel routing (*routing table*). Di mana tabel routing, informasi routing akan disimpan dalam bentuk *entry-entry route* (rute). Setiap entry route akan menunjukkan network address



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	172.16.1.1 reachable ether1	1		
DAo	10.10.10.0/24	192.168.1.1 reachable wlan1	110		
DAo	10.100.100.0/24	192.168.1.3 reachable wlan1	110		
DAC	172.16.1.0/24	ether1 reachable	0		172.16.1.2
DAC	192.168.1.0/24	wlan1 reachable	0		192.168.1.2
DAo	192.168.1.1	192.168.1.1 reachable wlan1	110		
DAo	192.168.1.3	192.168.1.3 reachable wlan1	110		
DAo	192.168.88.0/24	192.168.1.3 reachable wlan1	110		

8 items

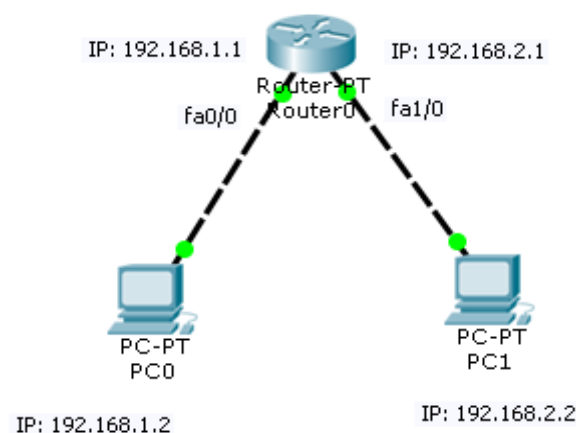
Gambar 34 Tabel Routing Router Mikrotik

dari network yang dapat dituju oleh router tersebut. Entry route ini juga berisi tentang informasi bagaimana cara mencapai network tersebut.

Entry route pada tabel routing di gambar 34 dapat di konfigurasi secara manual oleh Administrator jaringan atau dapat juga diperoleh router secara otomatis dengan melakukan pertukaran update routing dengan router lain.

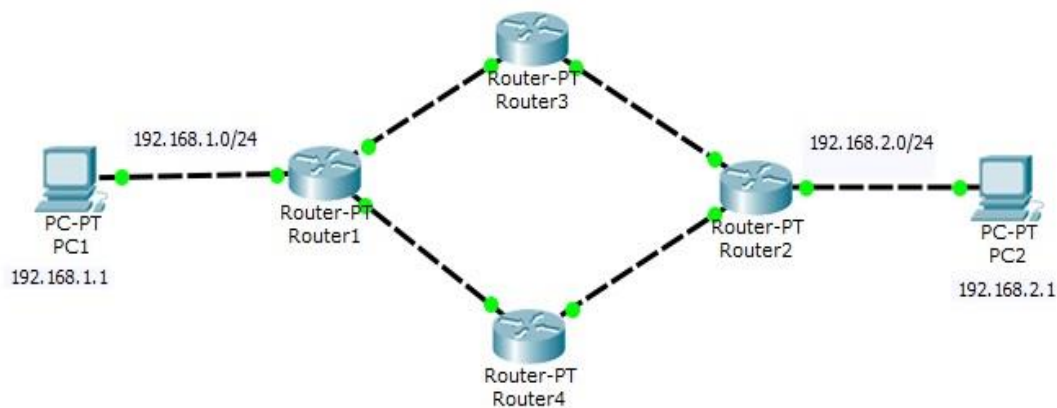
Teknik memasukkan entry route ke dalam router secara manual inilah yang disebut routing static (*static routing*), sedangkan teknik memasukkan informasi routing ke dalam tabel routing melalui pertukaran update routing dengan router lain disebut sebagai routing dinamic (*dynamic routing*). Pada dynamic routing, Administrator tidak akan memasukkan entry route secara manual ke dalam tabel routing.

Routing juga dapat menghubungkan beberapa jaringan yang terhubung langsung pada interface-nya, seperti terlihat pada gambar berikut ini. Pada jaringan tersebut tidak dibutuhkan teknik routing yang rumit karena merupakan jaringan yang sangat sederhana.



Gambar 35 Dua Network dihubungkan dengan sebuah Router

Namun routing juga dapat menghubungkan beberapa jaringan dengan menggunakan beberapa router seperti yang terlihat gambar 36. Tentu untuk jaringan yang rumit seperti itu dibutuhkan konfigurasi routing yang kompleks untuk menghubungkan client 192.168.1.1 dan client 192.168.2.1, karena diantara kedua host tersebut terdapat beberapa router.



Gambar 37 Client 192.168.1.1 memiliki pilihan jalur

7.2 Tabel Routing

Router berfungsi mengirimkan paket data dari satu network ke network lain sekaligus menentukan jalur terbaik (*best path*) untuk mencapai network tujuan. Untuk menjalankan fungsi tersebut router menggunakan tabel yang disebut tabel routing (*routing table*).

Tabel tersebut berisi informasi keberadaan beberapa network, baik network yang terhubung langsung (*directly connected network*) maupun network yang tidak terhubung langsung (*remote network*).

Tabel ini juga berisi informasi bagaimana cara router tersebut mencapai suatu network. Tabel routing ini sangat penting karena digunakan router sebagai pedoman untuk mengirimkan setiap paket data yang diterimanya.

Informasi dalam tabel routing berupa baris-baris *network address* yang disebut *entry route* (kadang cukup disebut router). Dalam setiap entry route juga telah ada informasi tentang interface mana yang dapat digunakan router tersebut untuk mengirimkan paket data. Jika router menerima paket data, maka router akan memeriksa IP address tujuan (*destination IP*) dari paket tersebut. Router kemudian mencocokkannya dengan *network address* yang ada pada setiap entry di tabel routing. Bila ada entry yang cocok maka router akan meneruskan paket tersebut ke interface yang digunakan untuk mengirimkan paket tersebut.

Interface yang digunakan untuk meneruskan paket tersebut disebut *exit interface* atau *outgoing interface*. Namun jika ternyata tidak ada entry yang cocok, maka router akan membuang (drop) paket data tersebut.

Ada empat kategori entry dalam tabel routing, yaitu :

1. Directly Connected Network

Entry ini akan muncul pada saat interface router diaktifkan dan dikonfigurasi IP Address. Beberapa jenis router status default dari interfacenya adalah disable (*non aktif*) sehingga perlu diaktifkan oleh Administrator jaringan. Pada router MikroTik, entry *Directly Connected* akan memiliki label C.

2. Static Routes

Entry ini adalah entry yang diisi manual oleh Administrator jaringan, sehingga jika terjadi perubahan jaringan, maka entry ini juga harus dirubah secara manual pula. Pada router Mikrotik, entry static route akan memiliki label S.

3. Dynamic Routes

Entry ini adalah entry yang akan muncul karena hasil pertukaran informasi routing dari beberapa router. Pertukaran informasi routing akan menggunakan routing protocol. Entry ini tidak diisikan manual oleh Administrator jaringan. Dalam hal ini Administrator hanya perlu mengaktifkan routing protokol dan network yang akan di routing. Pada router MikroTik, entry Dynamic Routes akan memiliki label D.

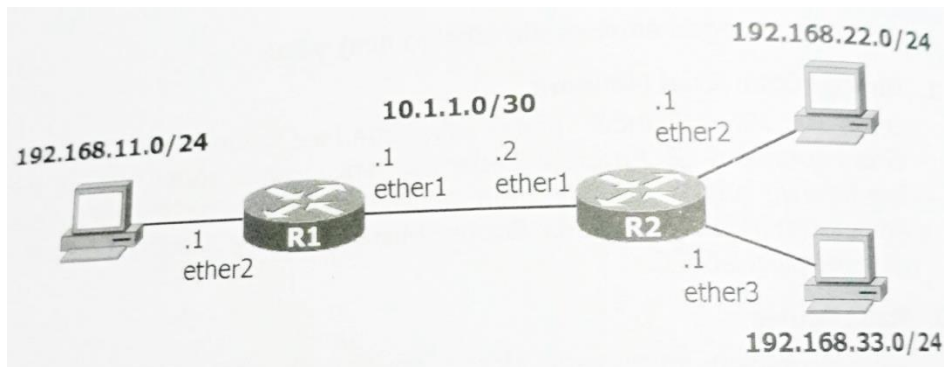
4. Default Routes

Entry ini digunakan untuk menentukan kemana sebuah paket akan dikirimkan jika alamat tujuan dari paket tersebut tidak terdapat pada tabel routing. Entry default routes bisa dikonfigurasi secara manual (static) ataupun di dapat dari pertukaran informasi dari routing protocol (dynamic). Entry default routes merupakan entry dengan nilai parameter *dst-address=0.0.0.0/0*. Jika dikonfigurasi secara static, maka default route akan memiliki label S.

Untuk dapat membaca dan memahami tabel routing dengan baik, Anda harus memiliki pengetahuan yang baik tentang mana network yang merupakan directly connected network dan mana yang merupakan remote network dari sebuah router.

Directly connected network adalah network atau jaringan yang terhubung langsung pada interface sebuah router. Sedangkan remote network adalah jaringan yang terhubung

langsung pada interface sebuah router. Untuk menjangkau remote network sebuah router membutuhkan router lain sebagai parameter next hop atau gateway.



Gambar 38 Router memiliki 2 remote network

Dari gambar diatas, Router R1 memiliki 2 (dua) directly connected network yaitu network 192.168.11.0./24 dan network 10.1.1.0/30.

Sedangkan untuk remote network, Router R1 memiliki 3 (tiga) directly connected network, yaitu network 192.168.22.0/24 dan 192.168.33.0/24.

Bagaimana dengan Router R2? Router R2 memiliki 3 (tiga) directly connected network, yaitu network 192.168.22.0/24 , 192.168.33.0/24 dan 10.1.1.0/30. Sedangkan untuk remote network, Router R2 hanya memiliki 1 (satu) remote network yaitu network 192.168.11.0/24.

Kita pelajari bagaimana bentuk dari tabel routing dan bagaimana router akan menggunakan tabel untuk mengirimkan paket data ke remote network. Tabel routing pastilah berisi network address directly connected, remote network dan bagaimana router itu menjangkau network-network tersebut.

Tabel routing tidak akan terbentuk sebelum Anda mengkonfigurasi IP Address pada interface router. Router R1 memiliki 2 (dua) interface dengan masing-masing memiliki IP Address 192.168.11.2/24 dan 10.1.1.1/30. Setelah IP Address dikonfigurasi maka tabel routing dari Router R1 akan terlihat seperti gambar di bawah ini.

```
[admin@R1] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 ADC  10.1.1.0/30        10.1.1.1      ether1        0
1 ADC  192.168.11.0/24     192.168.11.1  ether2        0
```

Gambar 39 Tabel routing Router R1

Gambar tabel routing diatas berisikan 2 (dua) entry route dan memuat beberapa parameter, yaitu :

- Dst-address, informasi yang ada dalam kolom ini menunjukkan network tujuan (destination) yang dapat di jangkau oleh router tersebut.
- Pref-src, menunjukan alamat IP address yang digunakan oleh router sebagai field IP address pengirim.
- Gateway, menunjukan cara router tersebut menjangkau network yang ada di kolom dst-address. Biasanya berupa interface ataupun IP Address dari router tetangga yang dapat digunakan untuk mencapai route network.
- Distance, menunjukkan nilai adminisrtratif Distance (AD) yang menunjukan seberapa besar nilai entry tersebut dapat dipercaya untuk digunakan. Niali ataupun dinamik, sekaligus dapat digunakan untuk melihat jenis routing protocol yang digunakan. Juga dapat digunakan untuk melihat apakah entry tersebut merupakan directly connected network.

Dari tabel routing tadi Anda dapat melihat jika Router R1 hanya mengenal network 192.168.11.0/24 dan 10.1.1.0/30. Router R1 sama sekali tidak mengenal kedua remote network 192.168.22.0/24 dan 192.168.33.0/24. Anda juga dapat melihat kode ADC di depan setiap entry yang berarti bahwa entry tersebut aktif (A) atau dapat digunakan.

Entry tersebut bersifat dinamik (D) karena di dapat router secara dinamik karena hasil konfigurasi IP Address pada interfacenya. Sedangkan inisial C di depan kedua entry tersebut menandakan bahwa kedua network merupakan directly connected network, atau network yang terhubung langsung.

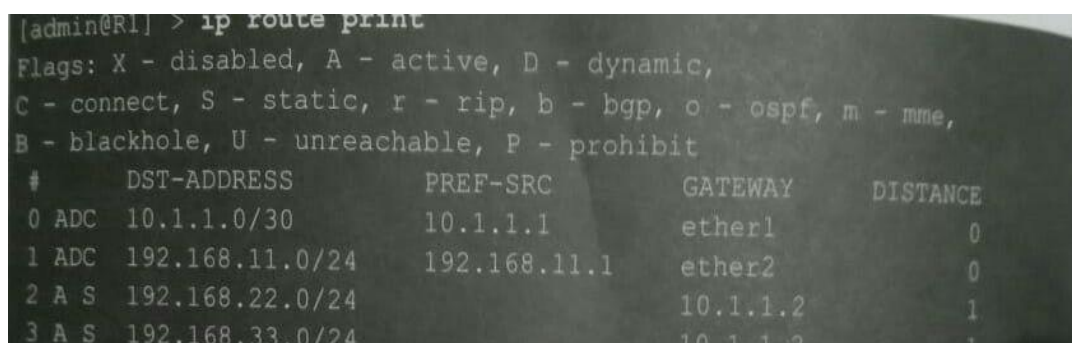
Pada kolom bagian parameter *gateway*, Anda juga dapat melihat bahwa yang digunakan untuk menuju network 10.1.1.0/30 adalah ether1 dan untuk menuju network, atau network 192.168.11.0/24 digunakan ether2. Karena kedua entry tadi merupakan directly connected network, maka nilai parameter *distance* keduanya adalah 0. Untuk benar-benar memahami tabel routing, gunakanlah selalu gambar topologi jaringan sebagai acuan.

Apa yang terjadi paket data yang ditunjukkan bagi network 192.168.22.0/24 atau network 192.168.33.0/24 ? Router R1 akan membuang paket data tersebut ini karena dalam tabel routingnya tidak terdapat entry dengan parameter *dst-address* 192.168.22.0/24 dan 192.168.33.0/24.

Router R2 belum mengenal keberadaan remote networknya 192.168.11.0/24. Ini mengakibatkan baik klien yang ada pada network 192.168.22.0/24 tidak dapat berkomunikasi dengan klien pada network 192.168.11.0/24.

Sekarang bagaimanakah agar Router R1 dan Router R2 mengetahui semua remote network mereka? Jawabannya adalah Anda harus menerapkan teknik routing pada kedua router tersebut. Anda dapat melakukannya dengan teknik routing statik maupun dinamik. Namun untuk mempelajari tabel routing pada bab ini, diasumsikan bahwa telah diterapkan teknik routing statik baik pada Router R1 maupun Router R2.

Dengan menggunakan routing static maka anda akan selaku Administrator jaringan harus memasukan sendiri remote network bagi setiap router. Anda harus memasukkan 2 (dua) entry remote network ke dalam tabel routing Router R1 dan 1 (satu) entry remote network ke dalam tabel routing Router R2. Setelah dikonfigurasi routing statik, maka tabel routing Router R1 akan terlihat seperti gambar dibawah ini.



```

[admin@R1] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#       DST-ADDRESS      PREF-SRC  GATEWAY      DISTANCE
0 ADC   10.1.1.0/30          10.1.1.1   ether1        0
1 ADC   192.168.11.0/24    192.168.11.1 ether2        0
2 A S    192.168.22.0/24              10.1.1.2      1
3 A S    192.168.33.0/24              10.1.1.2      1
  
```

Gambar 40 Tabel routing static pada Router R1

Gambar tabel Routing milik Router R1 diatas memperlihatkan bahwa router tersebut telah memiliki 2 entry tambahan untuk mengenal kedua remote networknya. Kedua entry memiliki label AS, yang artinya aktif (A) atau dapat digunakan dan keduanya merupakan entry yang didapat dari konfigurasi manual atau statik (S) dari Administrator jaringan, ditandai juga dengan nilai parameter distance sama dengan 1.

Terlihat pula bahwa Router R1 sudah mengenal keberadaan network 192.168.22.0/24 dan 192.168.33.0/24. Router R1 juga mengetahui bahwa untuk mencapai kedua network tersebut, dapat dilakukan melalui paarameter gateway= 10.1.1.2 yang merupakan IP address pada interface ether1 dari Router R2. Dengan kata lain Router R1 dapat mencapainya melalui Router R2.

Bagaimana dengan tabel routing R2 setelah dikonfigurasikan routing statik untuk remote network 192.168.11.0/24? Tabel routingnya dapat dilihat seperti gambar dibawah ini.

```
[admin@R2] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 ADC  10.1.1.0/30          10.1.1.2      ether1        0
1 A S   192.168.11.0/24      10.1.1.1      ether1        1
2 ADC  192.168.22.0/24      192.168.22.1  ether2        0
3 ADC  192.168.33.0/24      192.168.33.1  ether3        0
```

Gambar 41 Tabel routing statik pada Router R2

Pada gambar tabel routing Router R2 memperlihatkan bahwa router tersebut telah mengenal remote network 192.168.11.0/24 dan dapat di jangkau melalui parameter gateway=10.1.1.1 yang merupakan IP address pada interface ether1 milik R1 (Router R2 dapat mencapainya melalui Router R1).

Dengan lengkapnya tabel routing pada Router R1 dan Router R2, maka semua host akan dapat berhubungan dengan host lain, walaupun itu dengan host yang berbeda network.

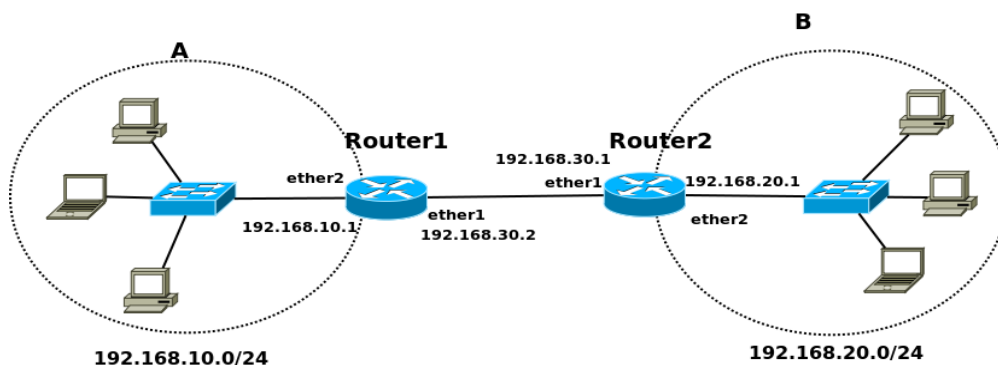
7.3 Routing Static

Routing statik atau static routing adalah teknik routing dimana entry routing pada tabel routing akan di susun oleh Administrator jaringan. Dengan kata lain, Anda sebagai

Administrator jaringan harus memilihkan jalur terbaik (best path) bagi router untuk menuju satu atau beberapa network tujuan.

Teknik routing ini memaksa anda untuk mengisi entry-entry routing secara manual, Entry-entry routing tersebut merupakan entry yang berisi network tujuan beserta gateway yang diperlukan untuk menuju network tujuan tadi.

Mari kita perhatikan contoh topologi sederhana pada gambar di bawah ini.



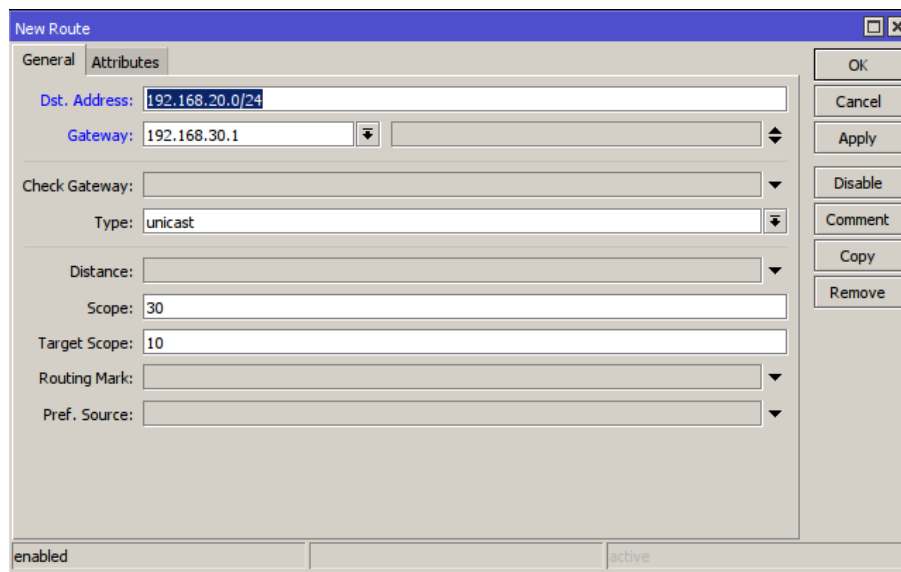
Gambar 42 Topologi jaringan 2 Router

Dari gambar diatas, terlihat bahwa Router1 memiliki network 192.168.10.0/24, sedangkan Router2 memiliki network 192.168.20.0/24. Kedua router tersebut dihubungkan oleh network 192.168.30.0/30 pada interface ether1 masing-masing router.

Masih pada gambar 42, Anda dapat melihat bahwa pada saat Router1 ingin menuju network 192.168.20.0/24, router tersebut harus menggunakan Router2 untuk next hop atau gateway. Lebih tepatnya lagi, Router1 harus menggunakan IP address 192.168.30.1 sebagai parameter gateway untuk menuju network 192.168.20.0/24.

IP Address 192.168.30.1 merupakan IP address yang ada pada interface ether1 milik Router2. Sehingga, agar Router1 dapat menjangkau network 192.168.20.0/24, maka konfigurasi routing pada Router1 harus terlihat seperti gambar di bawah ini. Perhatikanlah baris entry routing dengan parameter *dst-address*=192.168.20.0/24 dan *gateway*=192.168.30.1. Entry inilah yang dapat digunakan oleh Router1 untuk menuju network 192.168.20.0/24. Konfigurasinya sebagai berikut ini:

- Klik IP Router → Routes → Klik Tombol +



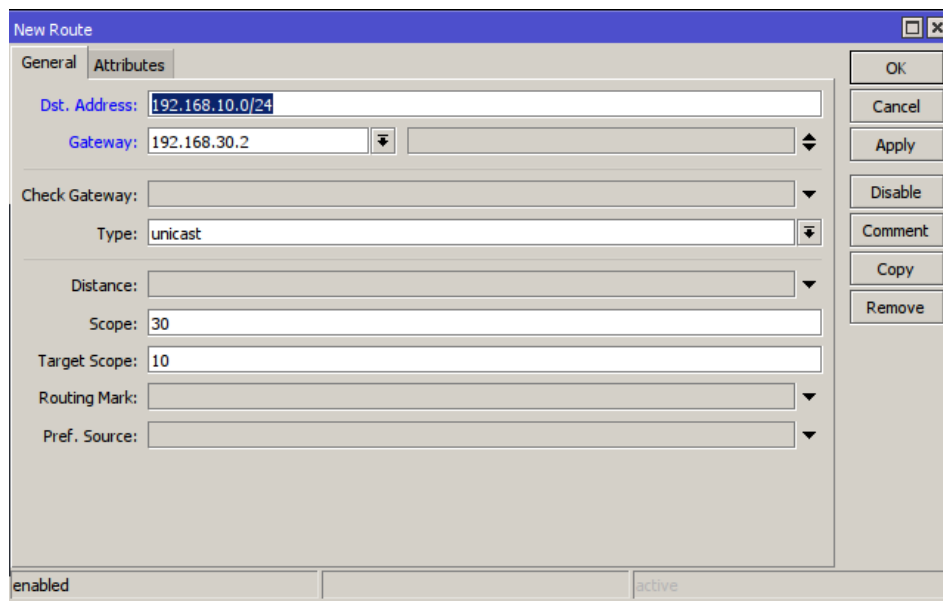
Gambar 43 Konfigurasi Static Routing pada Router1

- Perintah Command Linenya:

```
[admin@MikroTik]>/iproute add dst-address=192.168.20.0/24
gateway=192.168.30.1 type=unicast
```

Bagaimana dengan Router2? Router ini harus menggunakan Router1 untuk menuju network 192.168.10.0/14. Lebih tepatnya lagi, Router2 harus menggunakan IP Address 192.168.30.2 sebagai parameter gateway, dan IP address 192.168.30.2 tersebut merupakan ether1 milik Router1. Agar Router2 dapat menjangkau network 192.168.10.0/24, maka konfigurasi routingnya harus terlihat pada gambar di bawah ini. Perhatikanlah entry routing parameter *dst-address=192.168.10.0/24* dan *gateway=192.168.30.2*. Entry inilah yang digunakan Router2 untuk menuju network 192.168.10.0/24 yang berada dibelakang Router1. Konfigurasinya sebagai berikut:

- Klik IP Router → Routes → Klik Tombol +



Gambar 44 Konfigurasi Static Routing pada Router2

- Konfigurasi CLI:

```
[admin@MikroTik]>/ip route add dst-address=192.168.10.0/24
gateway=192.168.30.2 type=unicast
```

7.4 Routing Dynamic

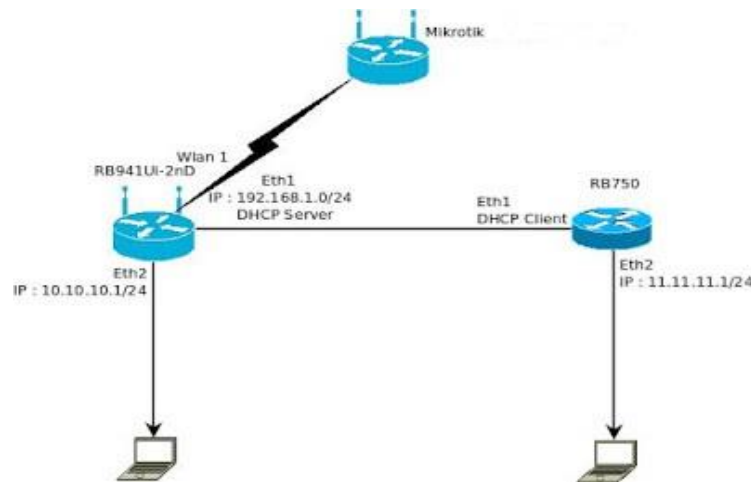
Routing dynamic atau dinamik routing merupakan routing yang memiliki dan membuat tabel routing secara otomatis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan antara router lainnya.

Diatur secara dinamis dengan menggunakan protokol routing, yaitu RIP (Routing Information Protocol), OSPF (Open Shortest Path First) dan BGP (Border Gateway Protocol). Dan perubahan dilakukan oleh router.

7.4.1 Routing RIP

RIP atau Routing Information Protocol yang merupakan routing protocol dengan algoritma distance vector, yang menghitung jumlah hop (*count hop*) sebagai routing metric. Jumlah maksimum dari hop yang diperbolehkan adalah 15 hop. RIP merupakan routing protocol yang paling mudah untuk di konfigurasi. Router-router yang menjalankan RIP akan saling bertukar informasi dengan router tetangganya (*neighbor*). Informasi yang dipertukarkan

adalah tabel routing miliknya, dengan kata lain sebuah router akan mengirimkan tabel routingnya ke neighbour router. Latar belakang mengapa dilakukan routing RIP, jika di jaringan pasti Anda memerlukan banyak mikrotik, maka konfigurasi mikrotik dengan static pasti memerlukan waktu yang lama, tetapi jika Anda menggunakan dinamic routing maka akan waktu pekerjaan. Dibawah ini topologi dasar untuk Routing RIP dan konfigurasinya.



Gambar 45 Topologi Routing RIP 2 Router

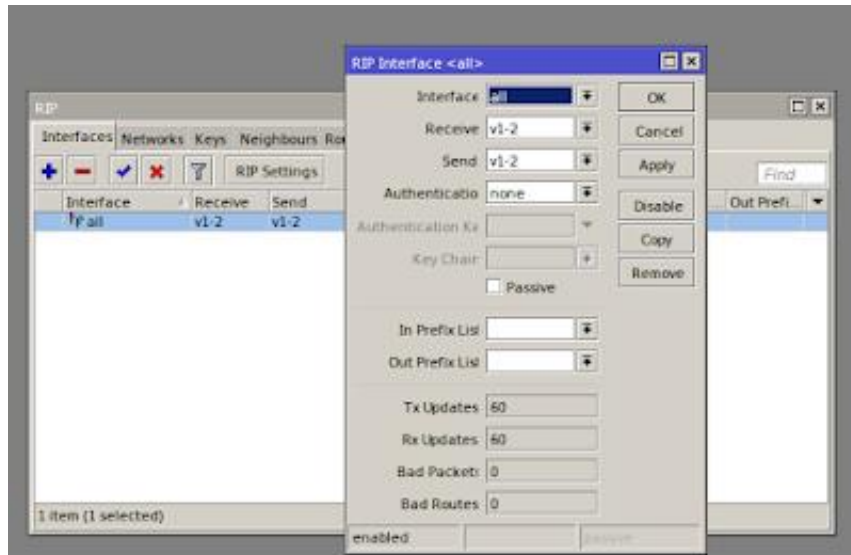
1. Konfigurasi Router 1

- Pertama pastikan bahwa router kita sudah ada sumber internetnya
- Kita konfigurasi IP Address nya seperti dibawah ini
- ether3 192.168.50.2/24 ==> ip yang terhubung ke router lain
- ether1 192.168.60.1/24 ==> ip yang digunakan untuk client

	Address	Network	Interface
D	192.168.43.183/24	192.168.43.0	wlan1
	192.168.50.2/24	192.168.50.0	ether3
	192.168.60.1/24	192.168.60.0	ether1

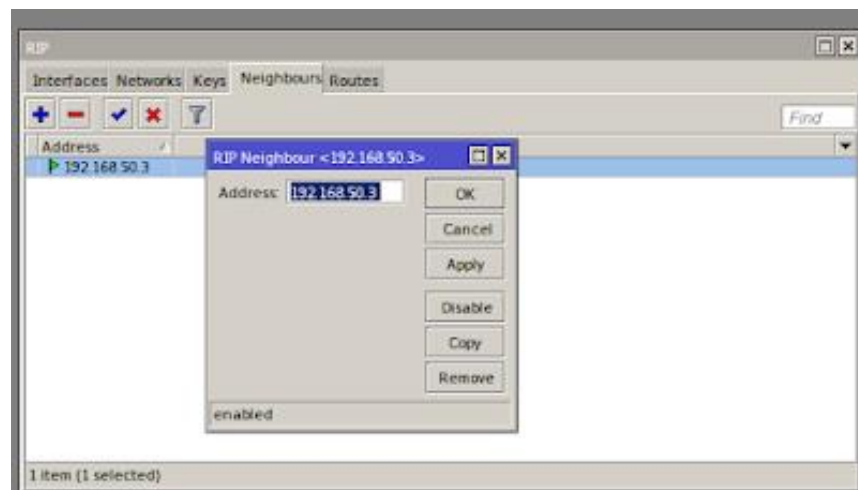
Gambar 46 Konfigurasi IP Address Router 1

- Setelah itu ke menu Routing → RIP
- Pada tab Interface klik + dan isi emtry seperti gambar dibawah ini
Lalu klik Apply → OK



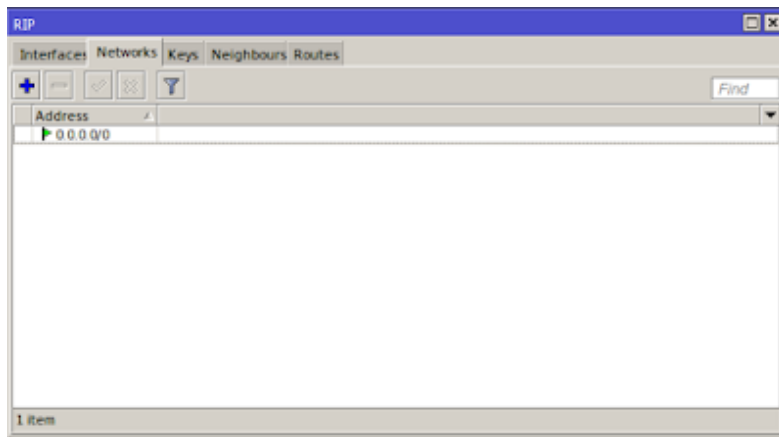
Gambar 47 Tab Interface Routing RIP Router1

- lalu kita pergi ke tab neighbours, kita klik simbol (+) lalu masukkan ip router lain yang terhubung ke Router 1 → klik Apply → OK



Gambar 48 Menambahkan IP router 2 yang terhubung ke Router1

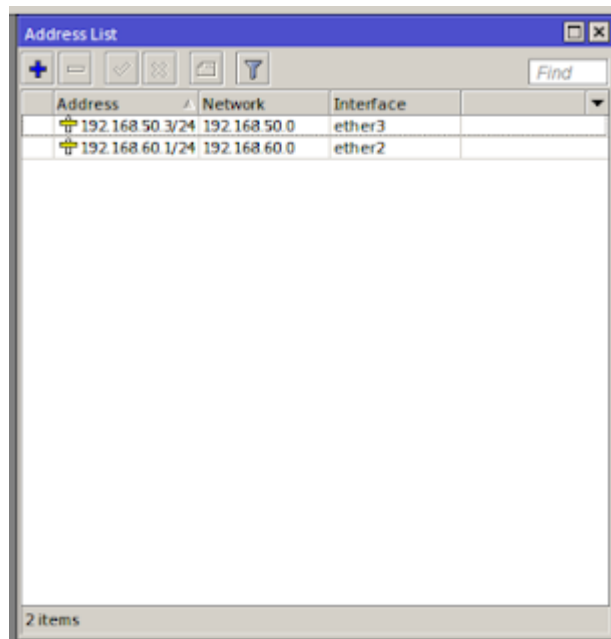
- lalu kita pilih ke tab network, kita klik simbol (+) lalu kita isikan 0.0.0.0/0 atau juga bisa kita berikan subnet yang terhubung ke mikrotik client 192.168.50.0/24, klik Apply → OK



Gambar 49 Input Network ke semua jaringan

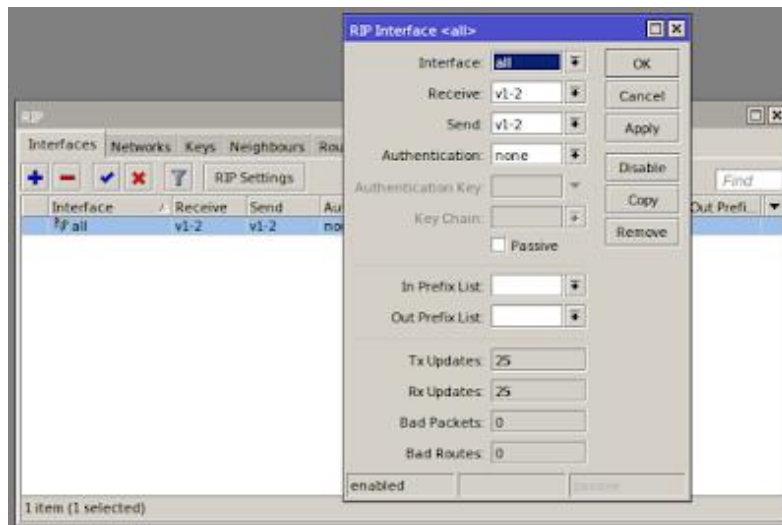
2. Konfigurasi Router 2

- kita setting ip address di menu IP → Address
- 192.168.50.3/24 ==> IP yang terhubung ke router lain
- 192.168.60.1/24 ==> IP yang digunakan untuk client



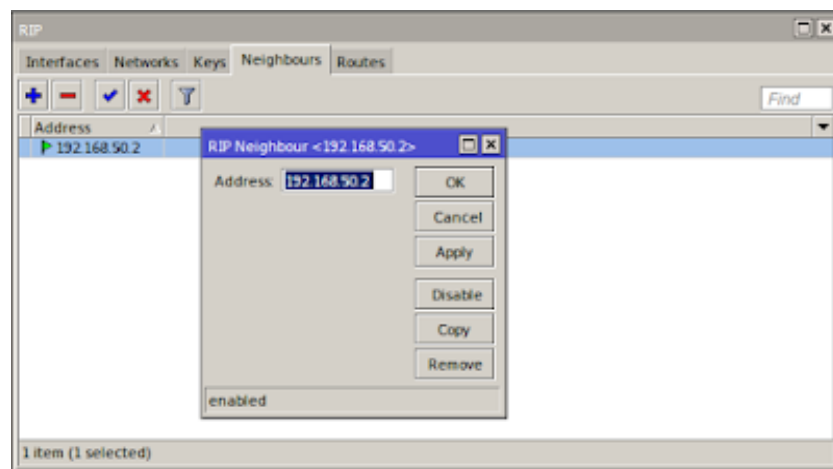
Gambar 50 Konfigurasi IP Address Router 2

- Klik Menu Routing → RIP
- di tab interface kita klik (+) lalu jika sudah kita konfigurasi kita klik Apply → OK



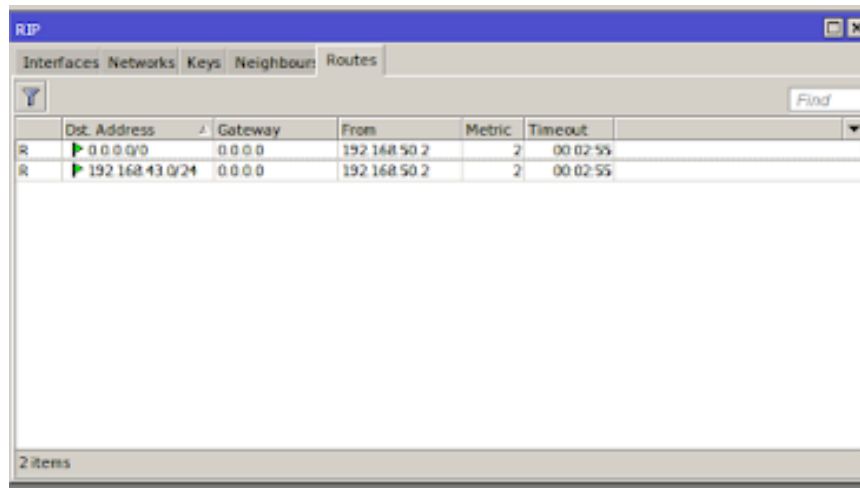
Gambar 51 Gambar 47 Tab Interface Routing RIP Router2

- o lalu kita pergi ke tab neighbours, kita klik simbol (+) lalu masukkan IP Router lain yang terhubung ke Router2 → klik Apply → OK



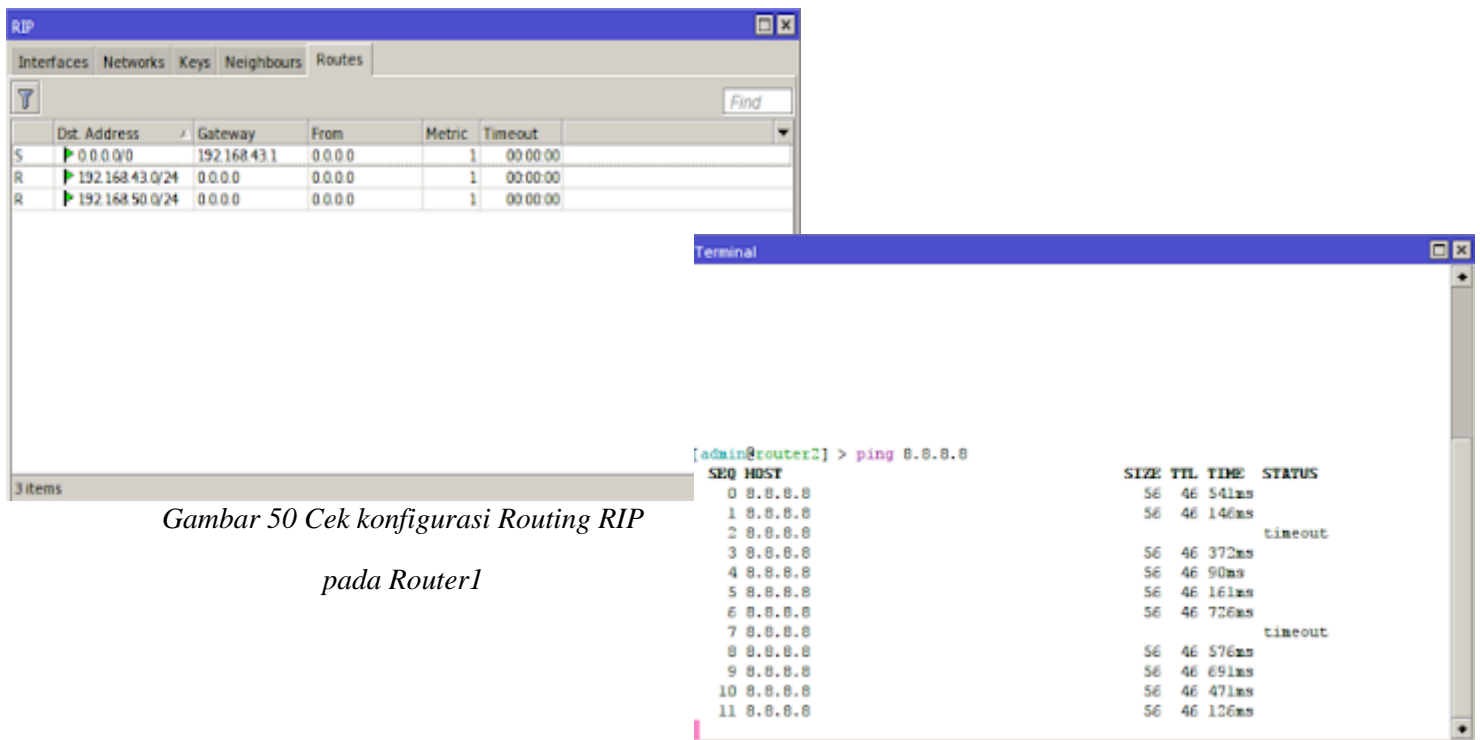
Gambar 48 Menambahkan IP Router1 yang terhubung ke Router2

- o cek Routes, jika berhasil maka hasilnya seperti gambar dibawah ini



Gambar 49 Konfigurasi Routing RIP pada Router2

- Pengecekan juga dilakukan di Router1 pada menu Routes
- Setelah pengecekan uji dengan melakukan ping 8.8.8.8 dari menu terminal



Gambar 50 Cek konfigurasi Routing RIP
pada Router1

Gambar 51 Cek Ping

7.4.2 Routing OSPF

OSPF (Open Shortest Path First) adalah sebuah protokol routing otomatis (*Dynamic Routing*) yang mampu menjaga, mengatur dan mendistribusikan informasi routing antar network mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah *Autonomous System (AS)* yaitu sebuah gabungan dari beberapa jaringan yang sifatnya routing dan memiliki kesamaan metode serta policy pengaturan network, yang semuanya dapat dikendalikan oleh network administrator. Dan memang kebanyakan fitur ini digunakan untuk management dalam skala jaringan yang sangat besar. Oleh karena itu untuk mempermudah penambahan informasi routing dan meminimalisir kesalahan distribusi informasi routing, maka OSPF bisa menjadi sebuah solusi.

OSPF termasuk di dalam kategori IGP (Interior Gateway Protocol) yang memiliki kemampuan Link-State dan Algoritma Dijkstra yang jauh lebih efisien dibandingkan protokol IGP yang lain. Dalam operasinya OSPF menggunakan protokol sendiri yaitu protokol 89. Umumnya OSPF diterapkan pada jaringan skala besar karena memiliki kemampuan untuk mencapai kondisi *convergence* yang sangat cepat, baik pada saat jaringan pertama kali dihidupkan maupun bila terjadi perubahan jaringan. Untuk dapat menangani jaringan yang berskala besar, maka OSPF menggunakan konsep area dalam implementasinya. Sehingga pengimplementasian OSPF dikenal dengan dua cara, yaitu Single Area OSPF dan Multi Area OSPF. Beberapa literatur menyarankan untuk menggunakan Multi Area OSPF bila jumlah router dalam jaringan OSPF sudah mencapai 50 router.

Berikut ini adalah sedikit gambaran mengenai prinsip kerja dari Routing OSPF :

- Setiap router membuat Link State Packet (LSP)
- Kemudian LSP didistribusikan ke semua neighbour menggunakan Link State Advertisement (LSA) type 1 dan menentukan DR dan BDR dalam 1 Area.
- Masing-masing router menghitung jalur terpendek (Shortest Path) ke semua neighbour berdasarkan cost routing.
- Jika ada perbedaan atau perubahan tabel routing, router akan mengirimkan LSP ke DR dan BDR melalui alamat multicast 224.0.0.6
- LSP akan didistribusikan oleh DR ke router neighbour lain dalam 1 area sehingga semua router neighbour akan melakukan perhitungan ulang jalur terpendek.

7.4.2.1 Konfigurasi Routing OSPF – Back Bone Area

OSPF merupakan protokol routing yang menggunakan konsep hirarki routing, dengan kata lain OSPF mampu membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan yaitu area.

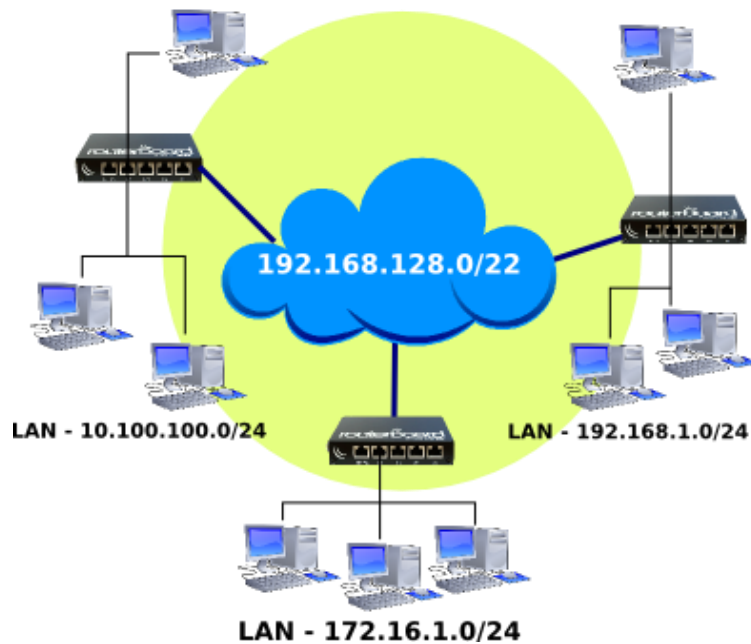
OSPF Memiliki beberapa tipe area diantaranya :

- Backbone - Area 0 (Area ID 0.0.0.0) → Bertanggung jawab mendistribusikan informasi routing antara non-backbone area. Semua sub-Area HARUS terhubung dengan backbone secara logikal.
- Standart/Default Area → Merupakan sub-Area dari Area 0. Area ini menerima LSA intra-area dan inter-area dari ABR yang terhubung dengan area 0 (Backbone area).
- Stub Area → Area yang paling "ujung". Area ini tidak menerima advertise external route (digantikan default area).
- Not So Stubby Area → Stub Area yang tidak menerima external route (digantikan default route) dari area lain tetapi masih bisa mendapatkan external route dari router yang masih dalam 1 area.



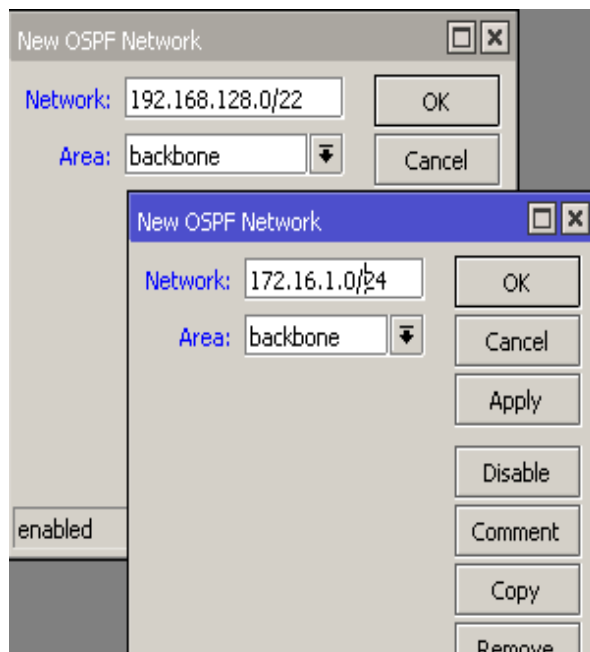
Gambar 52 ASBR, ABR dan IR

Kali ini kita akan mencoba melakukan implementasi untuk konfigurasi Backbone - Area 0 pada OSPF. Adapun langkah-langkahnya cukup mudah. Disini kami mempunyai 3 router dengan masing-masing router memiliki jaringan LAN. Kita akan mencoba supaya setiap jaringan LAN pada ketiga router tersebut bisa saling komunikasi tanpa kita tambahkan rule static route secara manual. Untuk gambaran topologi bisa dilihat pada tampilan dibawah ini.

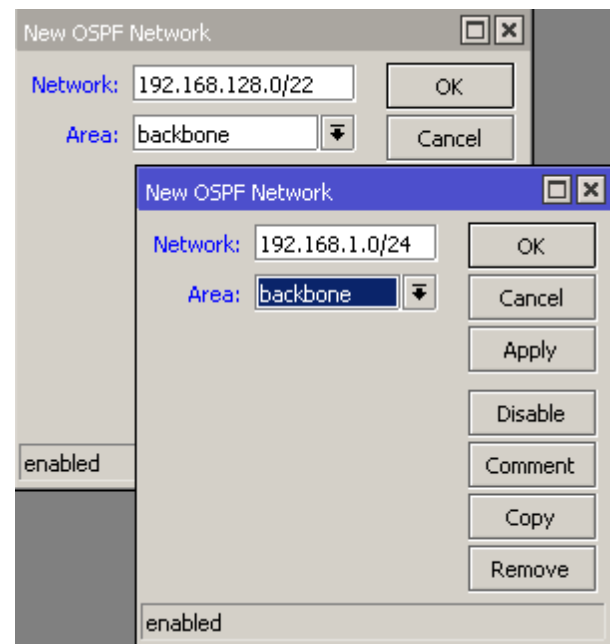


Gambar 53 Topologi Routing OSPF

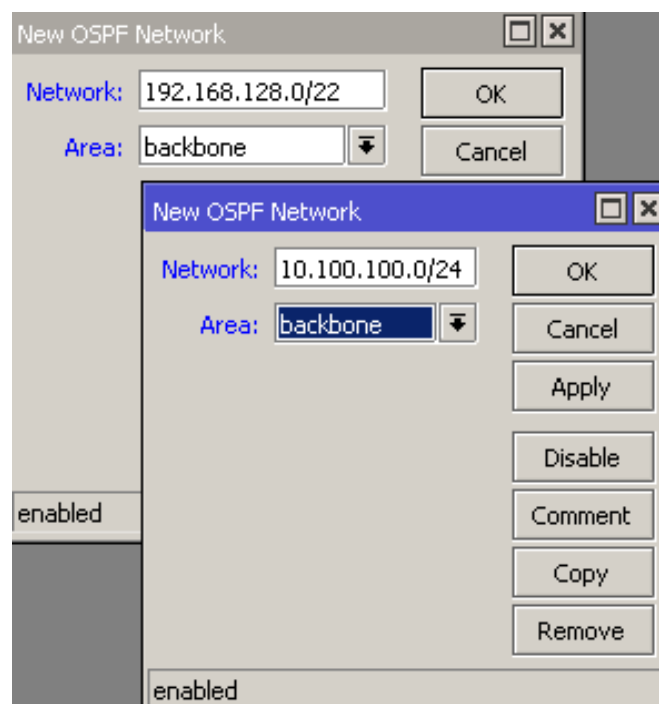
- Konfigurasi dari setiap router juga sama tidak ada perbedaan. Langkah awal Anda masuk pada menu Routing → OSPF → Network. Kemudian tambahkan network yang terdapat di router.



Gambar 54 Konfigurasi Network Routing OSPF Router1



Gambar 55 Konfigurasi Network Routing OSPF Router2



Gambar 56 Konfigurasi Network Routing OSPF Router3

- Setelah kita menambahkan network pada masing-masing router, jika kita melihat pada OSPF → Interfaces maka secara otomatis akan muncul interface router dimana network tersebut terpasang. Dengan kita menambahkan network itu secara otomatis pula OSPF pada masing-masing router telah aktif.
Pada menu IP → Routes juga akan ditambahkan secara dinamis rule routing baru dengan flag **DAo** (*Dinamic, Active, Ospf*).

Route List		
Routes	Nexthops	Rules
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>		
	Dst. Address	Gateway
AS	0.0.0.0/0	192.168.128.1 reachable ether1
DAo	2.2.2.0/24	192.168.128.10 reachable ether1
DAC	172.16.1.0/24	ether2 reachable
DAo	192.168.1.0/24	192.168.128.103 reachable ether1
DAC	192.168.128.0/22	ether1 reachable

Gambar 57 Hasil Konfigurasi Routing OSPF

- Lalu sampai pada langkah ini seharusnya jika Anda melakukan test ping maka setiap jaringan lokal sudah bisa reply. Dan berarti konfigurasi untuk OSPF Backbone (Area 0) telah selesai.

7.4.3 Routing BGP

Apabila kita berlangganan internet biasanya Provider Internet (ISP) mempunyai sebuah layanan untuk memisahkan jalur atau gateway antara koneksi internet Internasional dan OpenIXP. Dengan cara ini para customer dapat dengan mudah untuk melakukan management bandwidth untuk akses kedua jalur tersebut. Biasanya metode yang sering digunakan adalah dengan **BGP Peer**.

BGP (Border Gateway Protocol) adalah salah satu jenis protokol routing yang berfungsi untuk mempertukarkan informasi antar Autonomous System (AS). BGP ini merupakan sebuah Dinamic Routing dan pada mikrotik sendiri terdapat beberapa macam fitur dinamic routing

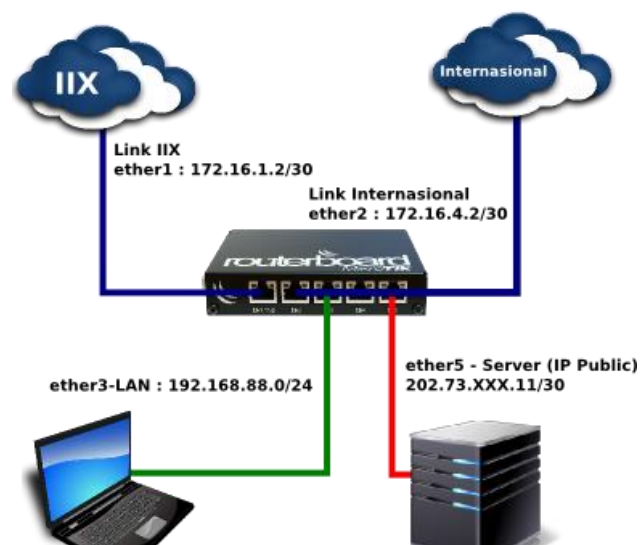
selain BGP seperti OSPF dan RIP. Untuk pertukaran informasi BGP ini memanfaatkan protokol TCP sehingga tidak perlu lagi menggunakan protokol jenis lain untuk menangani *fragmentasi, retransmisi, acknowledgement* dan *sequencing*.

Internet terdiri dari sekumpulan jaringan yang terhubung satu sama lain. Jaringan - jaringan tersebut bisa saja terdiri dari jaringan milik Internet Service Provider (ISP) maupun jaringan-jaringan skala enterprise.

Untuk menghubungkan jaringan antar ISP maupun antar ISP dengan enterprise network tadi dibutuhkanlah routing protocol yang handal. Saat ini, routing protocol yang digunakan untuk menghubungkan antara jaringan tersebut di internet adalah Border Gateway Protocol (BGP). Routing protocol ini mempunyai kelebihan dalam urusan menghubungkan jaringan-jaringan di Internet, yang tentunya merupakan jaringan berskala besar.

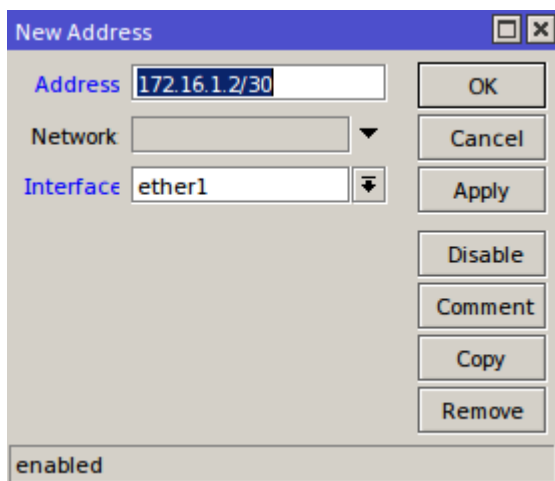
Untuk memahami bagaimana BGP digunakan dan bagaimana melakukan konfigurasi BGP maka Anda sebaiknya memahami juga bagaimana routing dilakukan di Internet. Harus dipahami dengan baik bagaimana router-router di Internet terhubung satu sama lain. Itulah sebabnya pada awal pembahasan bab ini, terdapat satu sub bab yang membahas routing di Internet. Ini bertujuan untuk memberikan gambaran awal bagaimana Routing BGP akan diterapkan.

Agar bisa mengetahui mengenai BGP lebih jauh lagi, kita akan langsung mencoba praktek konfigurasi BGP. Untuk percobaan kali ini kita akan memisahkan jalur dari koneksi internet Internasional dan IIX (lokal). Misal kita berlangganan internet pada sebuah ISP dengan layanan BGP Peer. Dengan contoh topologi seperti pada gambar berikut dan konfigurasinya.



Gambar 58 Topologi BPG Peer

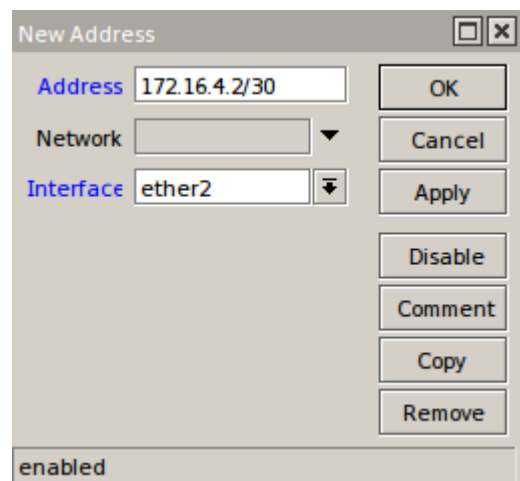
- Kita memiliki 2 (dua) buah link ke internet yaitu IIX dan Internasional yang menggunakan IP Local (172.16.1.2/30 dan 172.16.4.2/30) dengan satu link client local (192.168.88.0/24) dan satu link untuk server (menggunakan IP Public 202.73.XXX.11/30). Nah, masing-masing IP Address tersebut kita tambahkan pada interface router seperti pada topologi diatas.
- Semua IP Address ini hanya sekedar permisalan (*dummy*), jadi bisa disesuaikan dengan kondisi real implementasi di lapangan.



The 'New Address' dialog box shows the following configuration:

- Address:** 172.16.1.2/30
- Network:** (empty dropdown)
- Interface:** ether1
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status:** enabled

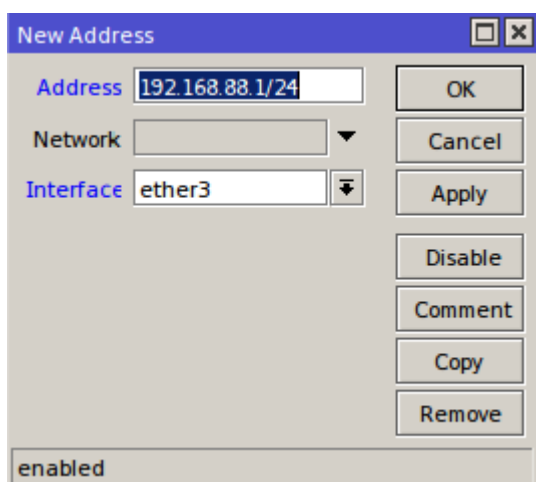
Gambar 59 Konfigurasi IP ether1 dari Internet



The 'New Address' dialog box shows the following configuration:

- Address:** 172.16.4.2/30
- Network:** (empty dropdown)
- Interface:** ether2
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status:** enabled

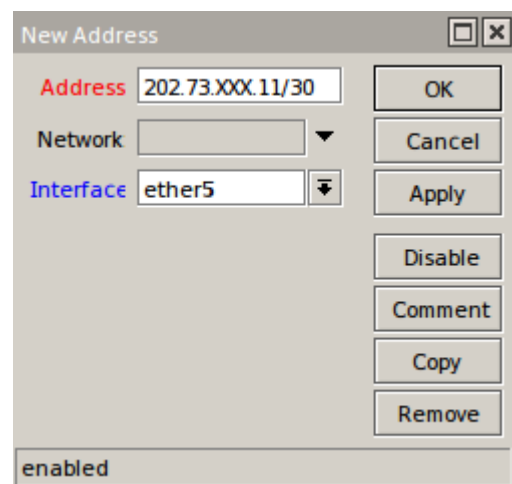
Gambar 60 Konfigurasi IP ether2 dari Internet



The 'New Address' dialog box shows the following configuration:

- Address:** 192.168.88.1/24
- Network:** (empty dropdown)
- Interface:** ether3
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status:** enabled

Gambar 61 Konfigurasi IP ether3 LAN

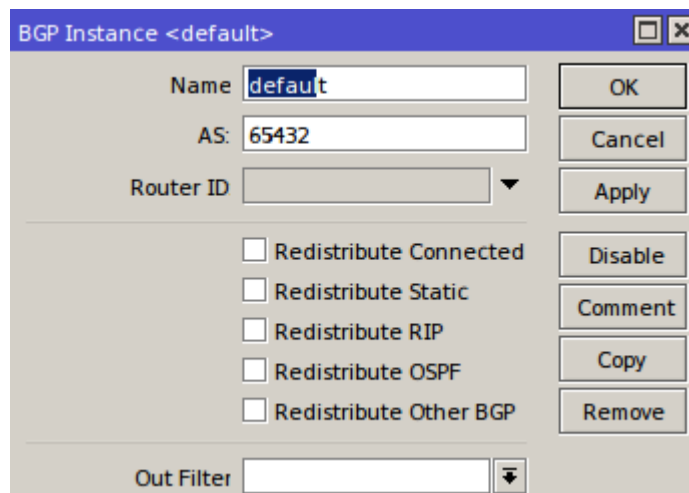


The 'New Address' dialog box shows the following configuration:

- Address:** 202.73.XXX.11/30
- Network:** (empty dropdown)
- Interface:** ether5
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status:** enabled

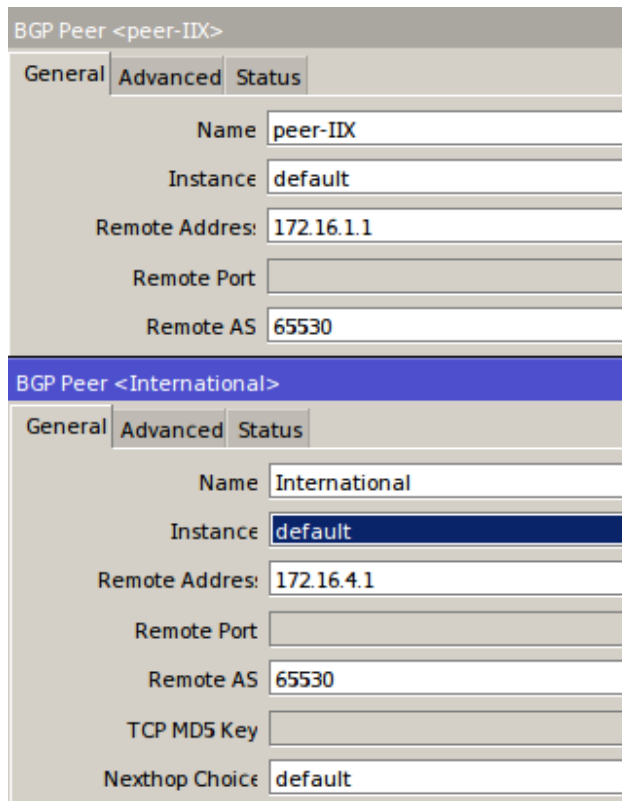
Gambar 62 Konfigurasi IP ether5 Public Network ke server

- Setelah itu tambahkan IP Address tersebut pada router, selanjutnya Anda akan melakukan konfigurasi pada menu BGP. Kita pilih pada menu Routing → BGP.
- Pada tab 'Instance' Anda tentukan nilai dari paramter AS (Autonomus System Number). Anda dapat menambahkan satu profile intsance baru atau Anda juga bisa mengubah konfigurasi pada profile yang telah ada (default). Nilai dari ASN ini kita sesuaikan dengan informasi dari ISP. Sebagai contoh disini kita menggunakan 65432.



Gambar 63 Konfigurasi Routing BPG Instance

- Kemudian Anda juga lakukan konfigurasi pada tab 'Peers'. Disini Anda akan menambahkan dua buah rule untuk *peering* (memasangkan) dengan BGP Router yang ada di ISP. Kita tambahkan peering untuk link koneksi Internasional dan juga IIX (lokal)



The image shows two screenshots of the Mikrotik WinBox BGP Peer configuration interface. The top screenshot shows the configuration for a peer named 'peer-IIX'. The bottom screenshot shows the configuration for a peer named 'International'.

Field	peer-IIX	International
Name	peer-IIX	International
Instance	default	default
Remote Address	172.16.1.1	172.16.4.1
Remote Port		
Remote AS	65530	65530
TCP MD5 Key		
NextHop Choice		default

Gambar 64 Menambahkan BGP Peer

- Pada parameter name Anda menentukan nama dari jenis koneksi tersebut (Internasional dan IIX). Kemudian Anda arahkan parameter instance ke profile yang telah dibuat sebelumnya yaitu 'default'. Untuk 'Remote Address' adalah gateway dari masing-masing link koneksi, Jangan lupa untuk menentukan 'Remote AS'. Hal ini juga disesuaikan dengan informasi dari ISP. Sebagai contoh kita kali ini kita menggunakan 65530.
- Apabila proses '*peering*' berhasil maka pada kolom state akan muncul keterangan '*Established*' dan jika kita melihat melalui New terminal dengan script `/routing bgp peer print`, maka pada dua rule yang kita buat tadi terdapat flag 'E'.


```

Terminal

+++++ Staff Support & Training - mikrotik.co.id +++++

[admin@MikroTik] > routing bgp peer print
Flags: X - disabled, E - established
#  INSTANCE  REMOTE-ADDRESS  REMOTE-AS
0  E default   172.16.4.1       65530
1  E default   172.16.1.1       65530
[admin@MikroTik] >

```

Gambar 65 Pengujian Peering

- Dan apabila Anda lihat pada menu **IP** → **Routes** maka akan muncul banyak sekali rule routing dengan flag '**DAb**' (Dynamic Active BGP) yang mana rule tersebut merupakan rule untuk destination dari IIX (lokal) dan juga Internasional.

Route List			
Routes			
Nexthops Rules VRF			
+ - ✓ ✗ [icon] [icon]			
	Dst. Address	Gateway	Distance
DAb	0.0.0.0/0	172.16.4.1 reachable ether2	20
DAC	10.10.10.0/24	wlan1 reachable	0
DAb	14.102.146.0/24	172.16.1.1 reachable ether1	20
DAb	14.102.150.0/24	172.16.1.1 reachable ether1	20
DAb	14.102.152.0/22	172.16.1.1 reachable ether1	20
DAb	23.0.166.0/23	172.16.1.1 reachable ether1	20
DAb	23.3.76.0/22	172.16.1.1 reachable ether1	20
DAb	23.5.192.0/20	172.16.1.1 reachable ether1	20
DAb	23.13.0.0/20	172.16.1.1 reachable ether1	20
DAb	23.37.192.0/20	172.16.1.1 reachable ether1	20
DAb	23.39.208.0/20	172.16.1.1 reachable ether1	20
DAb	23.39.224.0/20	172.16.1.1 reachable ether1	20
DAb	23.50.224.0/19	172.16.1.1 reachable ether1	20
DAb	23.51.0.0/20	172.16.1.1 reachable ether1	20
DAb	23.60.152.0/22	172.16.1.1 reachable ether1	20
1708 items			

Gambar 66 Tabel Routing BPG

- Sampai langkah ini IP Public yang ada pada router Anda sudah bisa diakses dari luar. Namun, untuk koneksi internetnya sendiri dari router maupun LAN (client) masih belum bisa diakses. Untuk itu kita akan menambahkan rule pada **firewall NAT**. Namun disini kita tidak akan menggunakan rule NAT dengan "**action=masquerade**", karena link yang menuju ke internet yaitu ether1 dan ether2 menggunakan *IP Private*. Sehingga kita akan menggunakan "**action=src-nat**" dengan menunjuk *IP Public* yang berada pada salah satu interface router yaitu di ether5.

- Pertama, kita tambahkan NAT untuk dua link koneksi ke internet (Internasional dan IIX). Contoh scriptnya adalah sebagai berikut:

```
[admin@MikroTik]> /ip firewall nat = add action=src-nat chain=srcnat  
out-interface=ether1 src-address=172.16.1.2 to-addresses=202.73.xxx.11  
add action=src-nat chain=srcnat out-interface=ether2 src-  
address=172.16.4.2 to-addresses=202.73.xxx.11
```

- Kedua, kita tambahkan NAT untuk akses internet dari jaringan LAN. Contoh scriptnya adalah sebagai berikut:

```
[admin@MikroTik]> /ip firewall nat add action=src-nat chain=srcnat src  
address=192.168.88.0/24 to-addresses=202.73.xxx.11
```

- Dari langkah ini seharusnya client maupun router sudah bisa koneksi ke internet. Kita bisa melakukan traceroute atau test ping untuk pengecekan. Demikianlah langkah-langkah bagaimana cara konfigurasi dasar dari BGP. Anda bisa sesuaikan alokasi ip addressing sesuai dengan kondisi real pada jaringan Anda.

DAFTAR PUSTAKA

1. Toto Harjendro, Modul Mikrotik. LP3T Nurul Fikri, 2015
2. Rendra Towidjojo, Mikrotik Kung Fu Kitab 2, Jasakom, 2016
3. Rendra Towidjojo, Mikrotik Kung Fu Kitab 4, Jasakom, 2016
4. <https://id.wikipedia.org/wiki/MikroTik>
5. <http://mikrotik.co.id/artikel>