

**RANCANG BANGUN DUAL LINK INTERNET SERVICE PROVIDER MENGGUNAKAN METODE
LOAD BALANCING DENGAN ALGORITMA ROUND ROBIN**

**DESIGN AND BUILD DUAL LINK INTERNET SERVICE PROVIDER USING LOAD BALANCING
METHOD WITH ROUND ROBIN ALGORITHM**

Muhamad Firdaus¹, Siti Madinah Ladjamuddin²

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
¹firdaus.m@gmail.com, ²citymadinah07@istn.ac.id

ABSTRAKSI

Perkembangan teknologi internet dimana para penggunanya yang menginginkan layanan yang selalu tersedia setiap saat semakin meningkat mengikuti perkembangan zaman yang biasanya belum tentu didukung dengan bertambahnya layanan iyang memadai. *Request* pengguna yang terlalu banyak menjadikan beban kerja pada *server* meningkat dengan cepat, mengakibatkan *server down* dalam waktu yang singkat serta dibutuhkan teknologi yang menangani penggunaan jaringan yang kompleks. Dalam jaringan komputer, *load balancing* adalah sebuah teknik untuk mendistribusikan beban kerja secara merata di dua atau lebih komputer, link jaringan, CPU, *hard drive*, atau sumber daya lainnya, untuk mendapatkan pemanfaatan sumber daya yang optimal, memaksimalkan *throughput*, meminimalkan waktu respon, dan menghindari *overload*. Dengan merancang *Load Balancing* pada *hotspot* warnet multi ISP (*Internet Service Provider*) sebagai sumber daya internet yang digunakan, diharapkan dapat memaksimalkan *throughput*, meminimalkan waktu respon dan menghindari *overload* penggunaan internet tersebut. Permasalahan pada saat ini adalah bila terjadi koneksi internet terputus maka tidak akan dapat mengakses aplikasi atau yang berhubungan internet. Untuk mengatasi hal tersebut, diperlukannya suatu koneksi internet alternatif sebagai fungsi berjalan di jalur koneksi yang sama dan dapat menggantikan koneksi utama bila terjadi masalah, sehingga akses internet tetap berjalan dengan baik.

Kata Kunci : *Load Balancing, ISP, Server, Jaringan, Failover*

ABSTRACT

The development of internet technology where its users who want services that are always available at all times are increasingly following the times that are usually not necessarily supported by the addition of adequate server services. Over-requests make the workload on the server increase rapidly, resulting in server down in a short time and needed technology that handles the use of complex networks. In computer networks, load balancing is a technique for distributing workloads evenly across two or more computers, network links, CPUs, hard drives, or other resources, to gain optimal resource utilization, maximize throughput, minimize response times, and avoid overload. By implementing Load Balancing on multi ISP internet café hotspots (Internet Service Provider) as internet resources used, it is expected to maximize throughput, minimize response time and avoid overloading internet usage. The problem at this time is that if there is an internet connection disconnected it will not be able to access applications or internet-related. To overcome this, the need for an alternative internet connection as a function to run on the same connection path and can replace the main connection in case of problems, while internet access continues to run properly.

Keyword : *Load Balancing, ISP, Server, Network, Failover*

1. PENDAHULUAN

Seiring berkembangnya teknologi informasi, internet menjadi kebutuhan manusia dalam segala aspek, terutama dalam dunia bisnis. Akses *internet* yang cepat dan stabil menjadi tuntutan dari meningkatkan kebutuhan penggunanya, hal ini tidak terlepas

dari peran sistem jaringan komputer pada perusahaan. (Leman, 2019)

Kebutuhan *bandwidth internet* semakin hari semakin meningkat, sehingga seringkali dibutuhkan penggunaan layanan *internet* dari beberapa ISP sekaligus. Sebuah perusahaan dapat menambahkan jalur *internet secondary*, jika merasa jalur *internet primary* tidak dapat menampung kebutuhan penggunaan

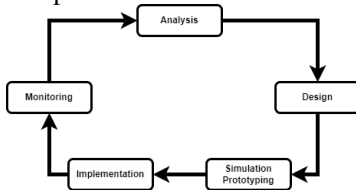
bandwidth secara maksimal. Pembagian penggunaan masing-masing jalur *internet* dapat diatur sesuai kebutuhan dan karakteristik pengguna. Penggunaan jalur-jalur *internet* juga dapat dimaksimalkan dengan penerapan teknik *load balancing*. (Leman, 2019)

Load balancing adalah sebuah teknik mendistribusikan beban *traffic* pada dua jalur atau lebih, sehingga didapatkan sambungan yang seimbang, *traffic* yang lebih optimal, *throughput data* maksimal, *delay* minimal, serta tidak terjadi *overload*. *Load balancing* dapat dirancang pada perusahaan yang memiliki minimal dua sambungan internet. Penelitian terkait menyatakan bahwa beban jaringan tidak menjadi lebih ringan dengan adanya *load balance*, akan tetapi *load balance* bertugas sebagai pengatur alokasi beban jaringan. *Load balancing* algoritma bekerja pada prinsip bahwa situasi di mana beban kerja diberikan, selama waktu kompilasi atau pada *runtime*. (Leman, 2019)

2. METODOLOGI PENELITIAN

Metode Rancang Bangun

Metode Rancang Bangun merupakan pengembangan sistem merupakan sebuah alternatif dalam mendalami suatu kajian ilmu. Metode pengembangan yang digunakan adalah NDLC (*Network Development Life Cycle*). Metode ini yaitu kunci dibalik proses perancangan jaringan komputer. NDLC merupakan model mendefinisikan siklus proses pengembangan sistem jaringan komputer.



Gambar Metode Rancang Bangun

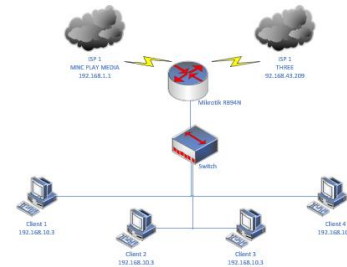
Pada Gambar Metode Rancang Bangun yang telah dirancang oleh penulis dapat dijelaskan alur proses perancangan jaringan sebagai berikut:

Analisa dan Perancangan

Pada tahap analisa dan perancangan penulis telah mendapatkan rician/rancangan spesifikasi yang akan dibangun. Pada tahap ini penulis akan membuat sebuah topologi jaringan dan sistem yang akan dibangun, agar dapat merancang *load balancing* dengan menggunakan metode algoritma *round robin* yang sudah dijelaskan pada bab sebelumnya.

Perancangan Fisik

Perancangan Fisik merupakan perancangan sebuah struktur jaringan yang berhubungan dengan peralatan yang digunakan dan pembentukan sebuah topologi jaringan. Perancangan ini bertujuan mempermudah dalam memahami struktur dan cara kerja *load balancing*. Selain itu juga bertujuan untuk *troubleshooting* jaringan, jika dalam pembangunan sistem masih terdapat beberapa kesalahan yang membuat *load balancing* belum dapat bekerja dengan baik. Gambar Topologi Sistem Load Balancing merupakan topologi jaringan yang akan dibangun dengan 1 mikrotik router dan 4 Client.



Gambar Topologi Sistem Load Balancing

Pada Gambar Topologi Sistem *Load Balancing* maka dapat dijelaskan sebagai berikut:

1. ISP 1 adalah *Internet Service Provider* yang disediakan oleh *provider* MNC Play Media dengan *gateway* 192.168.1.1
2. ISP 2 adalah *Internet Service Provider* yang disediakan oleh Telkomsel dengan *gateway* 192.168.43.209
3. Mikrotik yang digunakan adalah Mikrotik RB94N hap Lite, mikrotik ini digunakan untuk sistem *load balancing*, terdiri dari 4 port. Port 1 atau *ether1* terhubung dengan ISP1 (MNC Play Media), Port 2 atau *ether2* terhubung dengan ISP2 (Three), Port 3 atau *ether3* kosong, dan Port 4 atau *ether4* terhubung dengan Switch atau LAN.
4. Switch yang digunakan menyebarkan atau menjembatani untuk para *user*
5. Client 1 atau User 1 mendapatkan IP Address 192.168.10.3
6. Client 2 atau User 2 mendapatkan IP Address 192.168.10.4
7. Client 3 atau User 3 mendapatkan IP Address 192.168.10.5
8. Client 4 atau User 4 mendapatkan IP Address 192.168.10.6

Perancangan Logik

Perancangan logik adalah perancangan pemetaan proses perancangan konseptual dari perancangan fisik, memberikan pemetaan untuk IP Address dari setiap *hardware* atau alat yang digunakan

Berikut adalah tabel IP Address dari desain topologi yang sudah dibuat:

Tabel IP Address

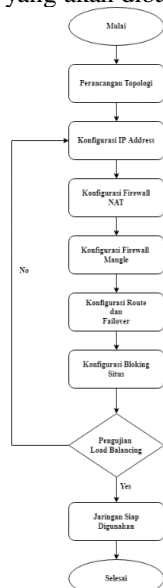
Perangkat	Interface	IP Address	Gateway
Mikrotik	ISP 1 (eth1)	192.168.1.2	192.168.1.1
	ISP 2 (eth2)	192.168.43.2	192.168.43.209
	Lokal (eth4) Mikrotik	192.168.10.2	172.168.10.1
Switch	Ethernet	-	-
PC Client 1	Ethernet	192.168.10.3	192.168.10.1
PC Client 2	Ethernet	192.168.10.4	192.168.10.1
PC Client 3	Ethernet	192.168.10.5	192.168.10.1
PC Client 4	Ethernet	192.168.10.6	192.168.10.1

Terdapat interface yang ada pada sisi router dengan penjelasan dari tabel diatas:

1. Interface ISP 1 : merupakan interface yang terkoneksi dengan jaringan yang berasal dar LAN menggunakan provider MNC Play
2. Interface ISP 2 : merupakan interface yang terkoneksi dengan jaringan yang menuju gateway ISP 2 yang berasal dari tethering menggunakan smartphone dengan provider Telkomsel
3. LAN (Local Area Network) atau Mikrotik merupakan Interface yang terkoneksi dari jaringan ISP 1 dan ISP 2, maka akan dikonfigurasi dan diterukan ke jaringan LAN
4. Interface Switch merupakan interface untuk mendistribusikan jaringan kepada seluruh pengguna atau client
5. Perangkat Client merupakan pengguna yang akan mendapatkan akses jaringan yang telah didistribusikan melalui menggunakan kabel LAN

Rancang Bangun Sistem Jaringan

Berikut adalah langkah-langkah yang dilakukan penulis untuk merancang sistem yang akan dibangun:



Gambar Diagram Rancang Bangun Sistem Jaringan

Pada Gambar Diagram Rancang Bangun Sistem Jaringan yang telah dibuat oleh penulis berawal dari membuat topologi jaringan dan instalasi hardware setelah itu maka dilakukan konfigurasi seperti konfigurasi IP address, Firewall NAT, Firewall Mangle, Routes & Failover dan melakukan konfigurasi blok situs. Setelah melakukan konfigurasi maka setelahnya dilakukakn pengujian, jika dalam dipengujian terdapat kegagalan maka proses dimulai ulang dengan dimulai dari konfigurasi IP, dan jika dalam pengujian berhasil maka jaringan siap dipakai oleh client.

Konfigurasi Load Balancing dengan Algoritma Round Robin

Algoritma Round Robin merupakan algoritma yang paling sederhana dan banyak digunakan oleh perangkat load balancing. Algoritma ini membagi beban secara bergiliran dan berurutan dari satu server ke server lain sehingga membentuk putaran. Metode yang selaras dengan Algoritma Round Robin adalah Metode Nth. Nth sendiri adalah sebuah fitur pada firewall yang digunakan sebagai penghitung (counter) dari paket data atau koneksi (packet new). Ada dua parameter utama dari Nth ini, yaitu "Every" dan "Packet". Berikut adalah tahapan yang harus dikerjakan untuk melakukan konfigurasi load balancing pada mikrotik.

Konfigurasi Dasar Load Balancing dengan metode Nth

Konfigurasi load balancing memerlukan beberapa tahapan, pertama melakukan konfigurasi dasar. Pada tahap pertama dilakukan adalah melakukakn konfigurasi interface yang digunakan sebagai jalur keluar masuk internet melalui router mikrotik. Setelah melalui pemeriksaan awal, kemudian menetapkan koneksi dengan ISP dan melakukan permintaan alamat IP (IP DHCP), kemudian melakukan konfigurasi IP Address pada masing-masing ethernet dan DNS yang akan digunakan.

Konfigurasi NAT (Network Address Translation)

Setelah melakukan konfigurasi dasar, selanjutnya harus melakukan konfigurasi NAT (Network Address Translation). NAT berguna supaya client dapat terhubung dengan internet. NAT akan mengubah alamat paket yaitu alamat client yang memiliki IP Address private agar dikenali oleh internet yaitu dengan cara mentranslasikan menjadi IP Address public. Pengaturan NAT menggunakan metode masquerading NAT. Karena provider yang digunakan hanya memberikan satu IP Address

public, jadi semua IP Address dari *client* akan dipetakan kepada satu IP *public*.

Tabel Perancangan konfigurasi NAT

Chain	Out Interface	Action
Srcnat	ISP 1	Masquerade
Srcnat	ISP 2	Masquerade

Konfigurasi Mangle

Mangle berguna untuk melakukan penandaan suatu paket, dimana penandaan yang dilakukan sesuai dengan kondisi dan syarat yang kita inginkan. Setelah itu hasil dari penandaan akan digunakan untuk kebutuhan tertentu berdasarkan *action* yang dipilih.

Konfigurasi Routing

Selanjutnya akan memetakan *route* atau jalur koneksi berdasarkan *routing mark* yang sudah dibuat pada konfigurasi *mangle*. *Routing mark* yang pertama akan menggunakan *gateway* dari ISP 1 dan *routing mark* yang kedua akan menggunakan *gateway* ISP 2.

Konfigurasi Failover

Failover berguna untuk menangani jika terjadi pemutusan koneksi pada salah satu jalur/ISP. Diharapkan sistem ini akan melakukan perpindahan *gateway* secara otomatis ke jalur yang tersedia atau aktif.

Fitur yang digunakan memanfaatkan proses pemeriksaan *gateway* dengan mengirimkan ICMP *echo request* kepada sebuah alamat yang dapat digunakan untuk mendeteksi kegagalan sebuah jalur. Dengan cara ini maka kegagalan jalur yang disebabkan oleh gagalnya *hop* dalam proses transaksi data juga dapat terdeteksi.

Konfigurasi Blocking Website

Konfigurasi *Blocking Website* pada penelitian ini bertujuan untuk memblokir situs-situs yang mengganggu penggunaan akses internet seperti mengganggu yang berpengaruh pada *bandwith*, dikarenakan situs-situs yang akan diblok terlalu banyak memakan *bandwith*. Selain itu juga untuk menjaga komputer terkena *virus* dari situs tersebut.

Langkah-Langkah Pengujian

Pada tahapan ini, penulis akan melakukan beberapa pengujian kinerja *load balancing* pada masing-masing metode diantaranya adalah sebagai berikut

1. *Availability* : Jika terdapat *server* (ISP) yang mati, maka *load balancer* akan menghentikan *request* ke *server* (ISP) tersebut dan mengalihkannya ke *server* (ISP) yang lain. Pengujian dilakukan dengan memutuskan koneksi ke salah satu *server* (ISP) secara bergantian.

2. *Balance* : Penulis akan menguji kinerja pada masing-masing metode *load balancing* dalam hal penyetaraan beban koneksi pada masing-masing jalur koneksi, baik pada ISP 1 maupun ISP 2. Pengujian dilakukan dengan dua cara, yaitu :

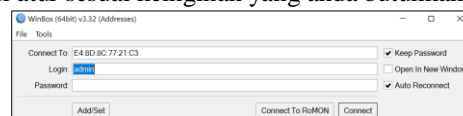
1. Dua *client* mengakses satu (1) *website*/situs yang sama, agar dapat dilihat pembagian jalur koneksinya. Apabila masing-masing *client* dapat mengakses situs tersebut melalui jalur *gateway* yang berbeda dari masing-masing *server*, maka *load balancing* sudah berjalan dengan baik.

Satu *client* mengakses situs yang sama melalui dua *browser* yang berbeda. Apabila jalur koneksi yang dilewatkan oleh *router* sebagai *load balancer* berbeda antara kedua *browser* tersebut, maka *load balancing* sudah berjalan dengan baik.

3. HASIL DAN PEMBAHASAN

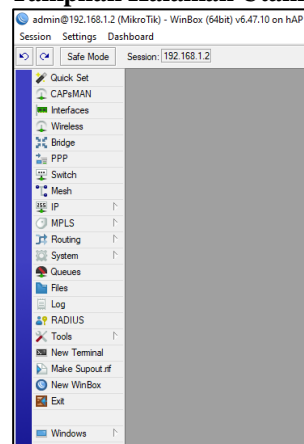
Login Winbox

Pada tahap awal ini kita akan menjalankan aplikasi *winbox* untuk *login* kedalam *Mikrotik* dengan IP, *Username*, dan *Password* yang bisa di atur sesuai keinginan yang anda butuhkan.



Gambar Login Winbox

Tampilan Halaman Utama Winbox



Gambar Tampilan Menu Utama Winbox

Pada Gambar Tampilan Menu Utama Winbox Setelah melakukan *login* kedalam aplikasi *mikrotik* maka akan menampilkan tampilan menu utama aplikasi *winbox* yang digunakan untuk melakukan semua konfigurasi yang dibutuhkan dalam suatu jaringan yang akan dibuat.

Pada tampilan utama *winbox* terdiri dari beberapa *tools* yaitu sebagai berikut.

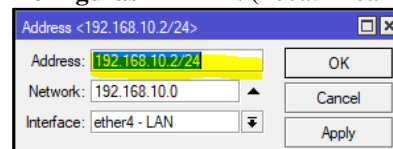
1. *Quick Set* digunakan untuk melakukan pengkonfigurasi mikrotik secara cepat.

2. *CAPsMAN (Controller Access Point sistem Manager)* merupakan sebuah fitur yang digunakan untuk memudahkan untuk mengatur semua perangkat *wireless* akses point yang ada di jaringan secara terpusat.
3. *Interface* merupakan sebuah fitur yang menampilkan gerbang trafik keluar dan masuk ke *mikrotik*. Nama *interface* dapat dirubah sesuai keinginan bertujuan untuk mempermudah dalam mengidentifikasi fungsi.
4. *Bridge* merupakan menu untuk menghubungkan dua segmen *network* terpisah bersama-sama dalam suatu protokol sendiri.
5. *PPP (Point to Point Protocol)*, merupakan paket yang memuat protokol *PPP*. Paket ini diperlukan untuk fitur komunikasi serial dengan menggunakan *PPP*, *ISDN PPP*, *L2TP*, dan *PPTP* serta komunikasi *PPP on Ethernet(PPPoE)*. Paket *PPP* digunakan untuk komunikasi *Wide Area Network* dengan menggunakan komunikasi serial
6. *Switch* Menu ini merupakan penghubung beberapa alat untuk membentuk suatu jaringan dalam lingkup kecil *Local Area Network*.
7. *Mesh* sebuah fitur untuk melakukan implementasi topologi jaringan *mesh*
8. *IP* digunakan untuk pengaturan *IP* dalam sebuah jaringan
9. *Routing* fitur ini berfungsi untuk membuat aturan atau alur jalan ke sebuah perangkat agar tidak terjadi permasalahan *link* atau koneksi.
10. *Sistem* fitur ini berfungsi untuk melakukan kontrol pada perangkat *mikrotik* itu sendiri.
11. *Queues* menu ini berfungsi untuk melakukan limit koneksi pada suatu jaringan baik berdasarkan *source address*, *destination address*, maupun berdasarkan paket yang telah dimark atau ditandai dari *mangle*, atau serta singkatnya bisa menggunakannya sesuai yang dibutuhkan.
12. *Files* menu ini berfungsi untuk menyimpan *file* dalam *OS Mikrotik* seperti *file-file HTML*, *login page hotspot*, *filebackup*, *file log* dan file lain yang kita ingin simpan dalam *OS Mikrotik*
13. *Log* menu ini memiliki fitur untuk melihat log aktifitas yang terjadi di *mikrotik*.
14. *Radius* merupakan protokol jaringan yang menjalankan *service management Authentication, Authorization, dan*

Accounting (AAA) secara terpusat untuk user yang terkoneksi dan hendak menggunakan *resource* dalam jaringan.

15. *Tools* adalah *root* menu dari beberapa *tools* yang dapat difungsikan yang ada pada *OS mikrotik*
16. *New Terminal* menu ini adalah fitur *console* pada *OS Mikrotik*

Konfigurasi IP LAN (*Local Area Network*)



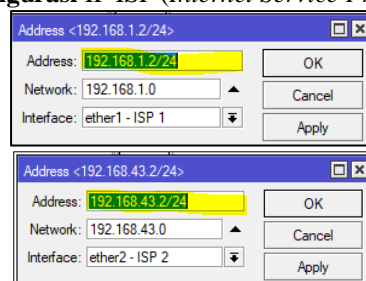
Gambar Konfigurasi IP LAN

Pada Gambar Konfigurasi IP LAN tahap ini penulis melakukan konfigurasi alamat IP Lokal atau LAN (*Local Area Network*) yang dibutuhkan agar *client* akan mendapatkan IP Address untuk *client* dapat terhubung ke jaringan.

Dibawah ini adalah langkah-langkah konfigurasi IP LAN:

1. Langkah pertama yaitu, Pada menu utama *Winbox* pilih menu IP lalu klik
2. Langkah kedua, Setelah klik, pilih *Addresses*
3. Langkah ketiga, Setelah itu klik *icon (+)* untuk menambahkan IP Address 192.168.10.2/24 pilih *interface* LAN.

Konfigurasi IP ISP (*Internet Service Provider*)



Gambar Konfigurasi IP ISP 1 dan ISP 2

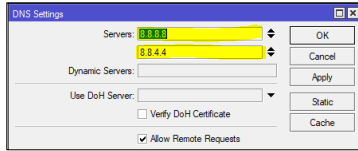
Pada Gambar Konfigurasi IP ISP 1 dan ISP 2, pada tahap ini dilakukan pemberian IP untuk kedua ISP (*Internet Service Provider*), yang bertujuan untuk memberikan IP agar *client* dapat terhubung dengan internet melalui dua ISP (*Internet Service Provider*) dengan jalur yang sama.

Untuk melakukan konfigurasi tersebut adalah sebagai berikut:

1. Langkah pertama, Pilih menu IP lalu klik
2. Langkah kedua, Setelah di klik, pilih *Addresses*
3. Langkah ketiga, Setelah itu klik *icon (+)* untuk menambahkan IP Address 192.168.1.2/24 dan pilih *interface ether1 - ISP 1*, kemudian *Apply* lalu *OK*

- Langkah keempat, Lalu klik icon (+) kembali untuk menambahkan IP Address ISP 2 192.168.43.2/24 dan pilih interface ether2 – ISP 2, kemudian Apply lalu OK

Konfigurasi IP DNS (Domain Name Server)



Gambar Konfigurasi IP DNS

Pada Gambar DNS (Domain Name Server) bertujuan untuk mencocokkan nama atau domain situs web ke dalam angka-angka yang disebut dengan alamat IP. Sehingga, komputer mengerti situs apa yang diminta.

Penyetingan DNS ini bertujuan untuk bisa terkoneksi pada google untuk melakukan testing pada jaringan yang telah dibuat.

- Langkah pertama, Pilih menu IP lalu klik
- Langkah kedua, Setelah masuk ke menu IP, Pilih DNS
- Langkah ketiga, Masuk ke DNS setting, lalu tambahkan DNS google yaitu 8.8.8.8

Konfigurasi NAT (Network Address Translation)

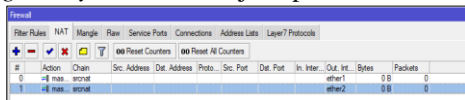
Untuk komputer client terhubung dengan internet, maka diperlukan translasi dari IP private yang dimiliki IP client ke IP public.

Tabel Konfigurasi Firewall NAT (Network Address Translation)

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1 - ISP 1 src-address=192.168.1.1/30

add action=masquerade chain=srcnat out-interface=ether2 - ISP 2 src-address=192.168.43.209/30
```

Pada baris pertama dalam perintah diatas merupakan perintah untuk masuk kedalam menu konfigurasi NAT (Network Address Translation). Setelah itu perintah tersebut mengintruksikan router agar mengganti sumber alamat IP dari sebuah paket ke IP public yang dimiliki interface “ISP1” dan “ISP2” dengan menggunakan metode masquerade, lalu paket dilemparkan ke gateway sesuai dari tujuan paket.



Gambar Konfigurasi NAT (Network Address Translation)

Konfigurasi Mangle

Untuk mengatur sebuah lalu lintas pada router mikrotik perlu dipastikan bahwa lalu lintas akan melalui interface yang sama dengan lalu lintas itu berasal. Untuk merekam aktivitas

koneksi harus menandai semua koneksi yang masuk.

Tabel Cammand Konfigurasi Firewall Mangle Mark Connection

```
/ip firewall mangle

add chain=prerouting in-interface=ether1 - ISP1 action=mark-connection new-connection-mark=Jalur 1

add chain=prerouting in-interface=ether2 - ISP2 action=mark-connection new-connection-mark=Jalur 2
```

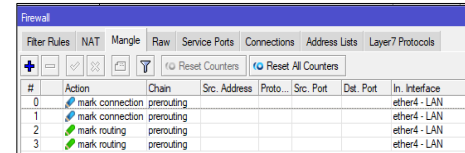
Setelah itu akan menetapkan mark routing untuk melihat seberapa berapa banyak paket yang keluar dari router pada masing-masing jalur. Mark routing dibagi sesuai dengan jalur yang ditentukan yaitu Jalur 1 dan Jalur 2.

Tabel Cammand Konfigurasi Firewall Mangle Mark Routing

```
add chain=prerouting connection-mark=Jalur 1 action=mark-routing new-routing-mark=ISP 1

add chain=prerouting connection-mark=Jalur 2 action=mark-routing new-routing-mark=ISP 2
```

Pada penelitian ini menggunakan dua 2 buah ISP, maka akan dibagi dengan dua (2). Kemudian hasil baginya akan digunakan sebagai penanda, maka koneksi tersebut akan ditandai sebagai “Jalur 1”. Kemudian dilewatkan ke routing mark “ISP 1” menggunakan gateway dari ISP1. Sedangkan jika koneksi tersebut akan ditandai sebagai “Jalur 2”, kemudian dilewatkan ke routing mark :”ISP 2” menggunakan gateway ISP2.



Gambar Hasil Konfigurasi Mangle

Konfigurasi Routing dan Failover

Untuk meneruskan paket yang telah ditandai dengan konfigurasi mangle, maka harus dibuat aturan baru pada routing tabel agar dapat melewati paket data tersebut ke gateway ISP (Internet Service Provider) yang sesuai dengan marking paket yang sudah dikonfigurasi pada tahapan konfigurasi mangle. Maka berikut ini adalah perintah untuk mengkonfigurasi pada routing table:

Tabel Cammand Konfigurasi Route dan Failover

```
/ip route

add dst-address=0.0.0.0/0 gateway=192.168.1.1 routing-mark=ISP 1 check-gateway=ping

add dst-address=0.0.0.0/0 gateway=192.168.43.209 routing-mark=ISP 2 check-gateway=ping

add dst-address=0.0.0.0/0 gateway=192.168.1.1 distance=1 check-gateway=ping

add dst-address=0.0.0.0/0 gateway=192.168.43.209 distance=1 check-gateway=ping
```

Untuk menentukan jalur koneksi diperintahkan untuk setiap *routing mark* dengan nama “ISP 1” akan selalu melalui *gateway* 192.168.1.1 dan untuk semua *routing mark* dengan nama “ISP 2” dengan *gateway* 192.168.43.209.

Fungsi pada parameter *distance* dalam konfigurasi tersebut untuk menentukan jalur *routing* mana yang akan menjadi prioritas dan yang menjadi jalur *backup*. Secara default nilai *distance* pada mikrotik dari 0 sampai 8. Semakin kecil nilai *distance* maka aturan tersebut akan semakin diprioritaskan. Berdasarkan konfigurasi *load balancing* dengan metode *nth*, ISP 1 dan ISP 2 memiliki prioritas yang sama dikarenakan memiliki nilai *distance*=1, maka dari itu ISP 1 dan ISP 2 saling *mem-backup* koneksi.

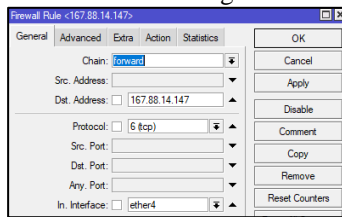
AS	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	192.168.1.1 reachable ether1 - ISP 1	1	ISP 1
AS	0.0.0.0/0	192.168.43.209 reachable ether2 - ISP 2	1	ISP 2
AS	0.0.0.0/0	192.168.1.1 reachable ether1 - ISP 1, 192.168.43.209 reach...	1	
DAC	192.168.1.0/24	ether1 - ISP 1 reachable	0	
DAC	192.168.10.0/...	ether4 - LAN reachable	0	
DAC	192.168.43.0/...	ether2 - ISP 2 reachable	0	

Gambar Konfigurasi Routing dan Failover

Kunci utama dari *failover* adalah pada pendefinisian *distance*. Dimaksudkan agar *routing* mendahulukan nilai *distance*, kemudian perintah “*add check gateway=ping*” bahwa *gateway* akan selalu dicek dengan cara melakukan *ping*, apakah hidup atau terputus. Jika *gateway* 192.168.1.1 tidak *me-reply*, maka *router* akan menganggap *gateway* 192.168.43.209 sebagai *gateway* dengan *gateway* dengan koneksi tunggal, dan berlaku juga untuk sebaliknya.

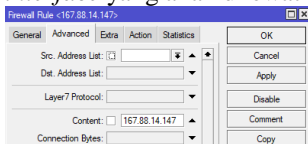
Konfigurasi Blocking Website

Pada tahap *blocking website*, penulis akan memblokir situs *streaming* ilegal Rebahin dengan menggunakan IP dari *website* tersebut, berikut adalah konfigurasi:



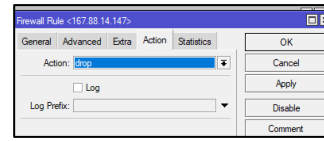
Gambar Pengaturan Firewall Rule General

Pertama-tama pilih tab *Filter Rules* kemudian tambahkan *Filter Rules* baru. *Chain* yang dipilih ialah *forward* kemudian *Src Address* diisi dengan *website* tujuan berupa IP *Addresses website* tujuan yang akan diblok yaitu 167.88.14.147 dan *In Interface* diisi dengan *interface* yang akan dilewati.



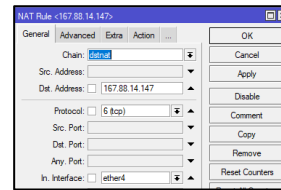
Gambar Pengaturan Firewall Rule Advanced

Kemudian pada *tab advanced*, isi *content* dengan IP *website* Rebahin yaitu 167.88.14.147



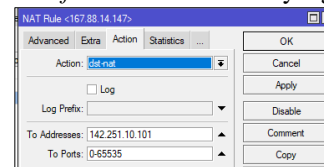
Gambar Pengaturan Firewall Rule Action

Pada tab *Action*, Pilih *Action* yaitu *drop* agar paket dari situs Rebahin diblok atau ditolak. Diatas adalah pengaturan bloknya tetapi untuk perlu mengalihkan *website* yang sudah diblok akan dialihkan ke *website* lain, untuk menglihkannya penulis menggunakan *website* www.google.com untuk mengalihkan situs yang diblok.



Gambar Pengaturan NAT Rule General

Pilih tab IP kemudian pilih tab *Firewall* lalu pilih NAT, Pada *chain* pilih *dstnat*, *dst*. *Address* masukan IP dari *website* yang diblok yaitu rebahin dengan IP 167.88.14.147, kemudian *Protocol* dipilih 6(tcp) dan *In*. *Interfaces* adalah *ether 4* yang akan dilalui



Gambar Pengaturan Firewall Rule

Pada tab *Action*, *Action* pilih *dst-nat*, kemudian pada *To. Addresses* masukan IP *website* pengalihan yaitu 142.251.10.101

Pengujian Load Balancing dengan Metode Nth

Pada tahap pengujian, penulis akan mengukur sejauh mana sistem yang telah dibangun dapat berjalan secara optimal. Cara pengujian adalah dengan melihat kerja sistem *load balancing* secara kualitas jaringan yang digunakan pada *load balancing*.

Pengujian Browsing

Pada tahap pengujian *browsing* akan menggunakan PC *Client* 1 dengan situs yang dituju yaitu www.youtube.com. Kegiatan pengujian ini sebagai contoh aktifitas *browsing* dari client.

Pada pengujian *load balancing* menggunakan metode *Nth*, sifat dasar dari *Nth* ini adalah *router* akan membagi jalur koneksi berdasarkan urutan antrian dari sumber yang ingin mengakses internet. Karena terdapat dua

koneksi atau dua ISP, maka antrian antrian yang dibuat sebanyak dua tersebut. Berikut ini adalah hasil dari monitoring koneksi yang terjadi ketika PC Client1 melakukan browsing pada situs www.youtube.com.

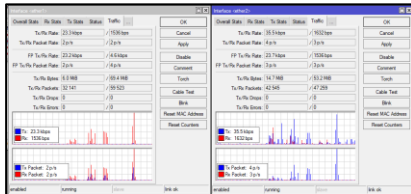
IP	Port	Connection Name	Status	Time
192.168.1.1	80	Client1	Success	10:00:00
192.168.1.1	80	Client1	Success	10:00:01
192.168.1.1	80	Client1	Success	10:00:02
192.168.1.1	80	Client1	Success	10:00:03
192.168.1.1	80	Client1	Success	10:00:04
192.168.1.1	80	Client1	Success	10:00:05
192.168.1.1	80	Client1	Success	10:00:06
192.168.1.1	80	Client1	Success	10:00:07
192.168.1.1	80	Client1	Success	10:00:08
192.168.1.1	80	Client1	Success	10:00:09
192.168.1.1	80	Client1	Success	10:00:10
192.168.1.1	80	Client1	Success	10:00:11
192.168.1.1	80	Client1	Success	10:00:12
192.168.1.1	80	Client1	Success	10:00:13
192.168.1.1	80	Client1	Success	10:00:14
192.168.1.1	80	Client1	Success	10:00:15
192.168.1.1	80	Client1	Success	10:00:16
192.168.1.1	80	Client1	Success	10:00:17
192.168.1.1	80	Client1	Success	10:00:18
192.168.1.1	80	Client1	Success	10:00:19
192.168.1.1	80	Client1	Success	10:00:20
192.168.1.1	80	Client1	Success	10:00:21
192.168.1.1	80	Client1	Success	10:00:22
192.168.1.1	80	Client1	Success	10:00:23
192.168.1.1	80	Client1	Success	10:00:24
192.168.1.1	80	Client1	Success	10:00:25
192.168.1.1	80	Client1	Success	10:00:26
192.168.1.1	80	Client1	Success	10:00:27
192.168.1.1	80	Client1	Success	10:00:28
192.168.1.1	80	Client1	Success	10:00:29
192.168.1.1	80	Client1	Success	10:00:30
192.168.1.1	80	Client1	Success	10:00:31
192.168.1.1	80	Client1	Success	10:00:32
192.168.1.1	80	Client1	Success	10:00:33
192.168.1.1	80	Client1	Success	10:00:34
192.168.1.1	80	Client1	Success	10:00:35
192.168.1.1	80	Client1	Success	10:00:36
192.168.1.1	80	Client1	Success	10:00:37
192.168.1.1	80	Client1	Success	10:00:38
192.168.1.1	80	Client1	Success	10:00:39
192.168.1.1	80	Client1	Success	10:00:40
192.168.1.1	80	Client1	Success	10:00:41
192.168.1.1	80	Client1	Success	10:00:42
192.168.1.1	80	Client1	Success	10:00:43
192.168.1.1	80	Client1	Success	10:00:44
192.168.1.1	80	Client1	Success	10:00:45
192.168.1.1	80	Client1	Success	10:00:46
192.168.1.1	80	Client1	Success	10:00:47
192.168.1.1	80	Client1	Success	10:00:48
192.168.1.1	80	Client1	Success	10:00:49
192.168.1.1	80	Client1	Success	10:00:50
192.168.1.1	80	Client1	Success	10:00:51
192.168.1.1	80	Client1	Success	10:00:52
192.168.1.1	80	Client1	Success	10:00:53
192.168.1.1	80	Client1	Success	10:00:54
192.168.1.1	80	Client1	Success	10:00:55
192.168.1.1	80	Client1	Success	10:00:56
192.168.1.1	80	Client1	Success	10:00:57
192.168.1.1	80	Client1	Success	10:00:58
192.168.1.1	80	Client1	Success	10:00:59
192.168.1.1	80	Client1	Success	10:01:00

Gambar Hasil Pengujian Browsing Pada Client 1

Hasil dari pengujian diatas, ditemukan bahwa saat mengakses situs www.youtube.com, mikrotik router membagi koneksi secara merata dan bergantian, hal ini terbukti dari jalur koneksi yang dilewatkan IP 192.168.1.2 bergantian dari Jalur 1 ke Jalur 2 secara berurutan.

Pengujian Keseimbangan Jaringan

Pada tahap ini *memonitoring* sistem jaringan dengan menggunakan *tools* yang berada di *winbox*. Ini adalah hasil dari monitoring yang berada di tab menu *interface list*:



Gambar Grafik Koneksi Gateway ISP1 dan ISP2 Parameter *traffic* yang dilihat pada gambar diatas adalah besar rata-rata dari penyebaran paket *transmitted* (Tx/Upload) dari setiap *gateway* masing-masing ISP. Dan pada gambar diatas penyebaran *packet* dan *bytes* yang hampir dikedua *interface*. Maka dari hasil ini dapat disimpulkan bahwa metode Nth dapat membagi penyebaran paket *transmitted* yang merata pada ISP 1 dan ISP 2.

Pengujian Kecepatan Jaringan

Pada tahap pengujian kecepatan jaringan, yaitu pengujian terhadap ISP 1 dan ISP 2 apakah kedua ISP tersebut sudah terhubung dalam satu jalur dan sudah menambah *bandwidth* baru dari kedua ISP tersebut.



Gambar Test Speed Dari ISP 1 dan ISP 2

Pada gambar 4.4.3 *Test Speed* Menggunakan ISP 1 dan ISP 2 merupakan jalur yang terdiri dari 2 ISP berbeda yang berada di satu jalur *load balancing*, maka dari *test speed* diatas adalah *bandwidth* dari ISP 1 ditambah dengan ISP 2 mendapatkan *bandwidth* yang lebih besar yaitu dengan *Download* 19,42 Mbps dan *Upload* 12,03 Mbps



Gambar Test Speed menggunakan ISP 1 MNC Play Media

Pada Gambar 4.4.4 *Test Speed* menggunakan ISP 1 MNC Play Media merupakan tes yang dilakukan hanya menggunakan ISP 1 saja, dengan ISP 1 *bandwidth* yang didapatkan yaitu *Download* sebesar 12,08 Mbps dan *Upload* sebesar 10,68 Mbps.



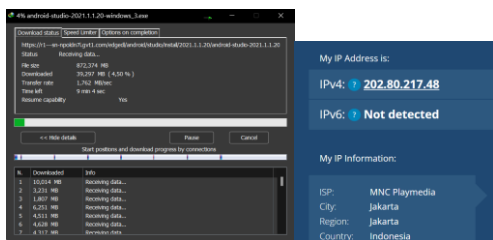
Gambar Test Speed menggunakan ISP 2 Provider TRI

Pada Gambar 4.4.5 *Test Speed* menggunakan ISP 2 *Provider TRI* merupakan tes yang dilakukan hanya menggunakan ISP 2 saja, dengan ISP 2 *bandwidth* yang didapatkan yaitu *Download* sebesar 5,61 Mbps dan *Upload* sebesar 5,48 Mbps.

Maka dapat disimpulkan bahwa dengan menggunakan sistem *load balancing dual link* ISP bahwa ketika sistem berjalan akan memberikan penambahan *bandwidth* dari masing-masing ISP.

Pengujian Failover

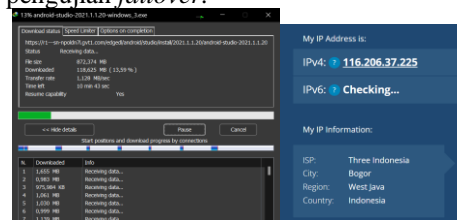
Pada tahap pengujian *failover*, yaitu pengujian terhadap masing-masing *load balancing*, untuk mengetahui kinerja *failover* dari sistem yang sudah dibangun. Fungsi dari *failover* adalah untuk mengatasi terjadinya terputus koneksi dari salah satu ISP. Dengan *failover* ini, apabila salah satu koneksi ISP terputus, maka masih memiliki satu ISP sebagai *backup* koneksi yang putus internet.



Gambar Pengujian Download Menggunakan Kedua ISP

Pengujian diatas dilakukan dengan *download* file dengan ukuran yang cukup besar melalui PC Client 1 menggunakan aplikasi *download manager* yaitu IDM (*Internet Download Manager*), yaitu dengan kondisi kedua ISP tersebut terkoneksi dengan *router* mikrotik. Pada saat proses *download gateway* awal adalah 202.80.217.48, IP tersebut adalah IP koneksi dari ISP 1 yaitu MNC Play.

Pada saat melakukan *download* berikutnya, penulis mencoba memutuskan jalur koneksi internet dari ISP1 yang sebelumnya terhubung ke *router* mikrotik. Berikut adalah hasil dari pengujian *failover*:

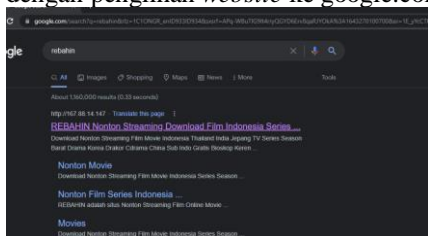


Gambar Pengujian Download Dengan ISP 1 Terputus

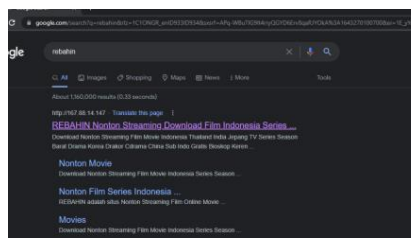
Dari pengujian tersebut, maka hasil yang diperoleh adalah *download* tetap berjalan tanpa mengalami gangguan koneksi dikarenakan ISP 2 akan secara *default gateway* yang dimana untuk mem-*backup* kinerja dari jaringan. Dengan ISP 1 terputus maka ISP 2 akan menjadi *default gateway* yaitu 116.206.37.225.

Pengujian Blocking Website

Setelah melakukan konfigurasi *blocking website* penulis melakukan pengujian *blocking website*. *Website* yang diblokir adalah *website streaming* film ilegal yaitu *Rebahin* dengan pengalihan *website* ke google.com.



Gambar Akses Website Rebahin
 Pada Gambar Akses *Website* Rebahin, penulis melakukan akses untuk menuju *website streaming film* Rebahin.



Gambar Pengalihan Website

Pada Gambar Pengalihan Website, ketika penulis melakukan akses kesitus Rebahin maka situs Rebahin tidak akan terbuka dan situs tersebut akan dialihkan kembali kesitus www.google.com.

4. SIMPULAN

Kesimpulan yang didapat setelah melakukan penelitian adalah sebagai berikut:

1. Merancang sistem *load balancing dual link Internet Service Provider* menggunakan metode algoritma *round robin* dengan menggunakan dua ISP berbeda dengan menggabungkan dua jalur tersebut menjadi satu jalur yang sama perancangan ini telah sesuai apa yang telah diharapkan oleh penulis.
2. Dengan metode *Nth load balancing* dua *gateway* digunakan secara bergantian yang sesuai dengan algoritma *round robin*. Sistem yang dibangun juga dapat membagi jalur koneksi secara merata atau berimbang berdasarkan *packet request*.
3. Sistem yang dibangun menggunakan metode *Nth load balancing*, sudah dapat menyelesaikan masalah, ketika dari salah satu ISP mengalami kendala/terputus. Dapat dilihat dari pengalihan koneksi secara otomatis ke *gateway* dari ISP yang masih aktif, maka kinerja jaringan tetap berfungsi.
4. Dengan memblokir situs tertentu maka pengguna tidak dapat membuka situs yang telah diblokir dan situs tersbut teralihkan ke situs yang lain.

Saran

Berdasarkan kesimpulan diatas, maka penulis mengajukan beberapa saran untuk pengembangan lebih lanjut dari penelitian yang telah dilakukan, yaitu:

1. Menambahkan konfigurasi *bandwith* supaya membagi *bandwith* secara merata sesuai jumlah *client* yang aktif.
2. Lebih disarankan untuk memilih ISP dengan *connection speed* dan *bandwith* yang sama untuk menghindari *browsing* yang lambat dikarenakan memiliki *response time* yang berbeda.

3. Untuk pengembangan selanjutnya *Load balancing* dapat lebih dikembangkan dengan mengguakan lebih dari dua ISP.

5. DAFTAR PUSTAKA

- [1] Leman Dedi, 2019. Load Balancing 2 Jalur Internet Menggunakan Mikrotik Round Robin.
- [2] Aini, N. (2019). Analisis Jaringan Local Area Network. 5(1). <https://doi.org/10.31219/osf.io/htxwe>
- [3] Ardhi Permana, M., Supendar, H., Informatika, T., Nusa Mandiri, S., Jl Jatiwaringin No, J., & Timur, J. (n.d.). Analisa Kinerja Load Balancing Terhadap Jaringan Local Area Network Berbasis Cisco Router. In Jurnal (Vol. 2, Issue 2). <http://ejournal.bsi.ac.id/ejurnal/index.php/infotech204>
- [4] Ardianto, F. (2020). Penggunaan mikrotik router sebagai jaringan server. Penggunaan Router Mikrotik, 1, 26–31.
- [5] Izzaty, R. E., Astuti, B., & Cholimah, N. (2021). SISTEM PENYARING SITUS SITUS TERLARANG BERBASIS MIKROTIK DENGAN FITUR FIREWALL PADA WLAN (STUDI KASUS GEDUNG KULIAH VI POLITEKNIK NEGERI SRIWIJAYA). Angewandte Chemie International Edition, 6(11), 951–952., 2006, 5–24.
- [6] Leman, D. (2019). LOAD BALANCING 2 JALUR INTERNET MENGGUNAKAN MIKROTIK ROUND ROBIN. In Riau Journal of Computer Science (Vol. 05).
- [7] Mair, Z. R., & Ariska, D. T. (2018). Optimalisasi Kinerja Jaringan Komputer Berbasis Router Kabupaten Musi Banyuasin. Jurnal Teknologi Informasi Dan Komputer Politeknik Sekayu, 8(1), 46–54.
- [8] Mohammad Badrul, A. (2019). Implementasi Automatic Failover Menggunakan Router Jaringan Mikrotik Untuk Optimalisasi Jaringan. Jurnal PROSISKO, 6(2), 82–87.
- [9] Nurnaningsih, D., & Permana, A. A. (2018). RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES). JURNAL TEKNIK INFORMATIKA, 11(2), 177–186. <https://doi.org/10.15408/jti.v11i2.7811>
- [10] Paratan, M. (2020). Analisis Sistem Keamanan Jaringan Hot-Spot. MERSI PARATAN.
- [11] Prayitno, M. H., & Lubis, H. (2020). Penerapan Logical Unit Number (LUN) Pada Drobo Virtual Storage Dengan Metode Network Development Life Cycle (NDLC). Explore: Jurnal Sistem Informasi Dan Telematika, 11(1), 45. <https://doi.org/10.36448/jsit.v11i1.1458>
- [12] Rahmah, R. D., Sari, A. P., Informasi, S., Fakultas, A., Bina, U., Informatika, S., Barat, J., Informasi, S., Teknik, F., Bina, U., & Informatika, S. (2021). IMPLEMENTASI WEB PROXY MENGGUNAKAN ROUTER MIKROTIK PADA dan internet sangatlah pesat . Hampir di setiap jaringan komputer untuk mempermudah arus informasi dalam perusahaan tersebut , sehingga bagi para penggunanya adalah komunikasi jaringan . Web Proxy se. 1(11), 298–306.
- [13] Sayah, F. (2019). Implementasi Load Balancing Dengan Metode Nth Pada CV. Pex's Cargo & City Courier Service. November, 21.
- [14] Supriyanto, A. (2018). Analisis Kelemahan Keamanan pada Jaringan Wireless. Analisis Keamanan Jaringan Wireless, XI(1), 38–46.