

# IMPLEMENTASI *FAIL OVER* MENGGUNAKAN JARINGAN VPN DAN METRONET PADA ASTRIDOGROUP INDONESIA

## *VPN FAILOVER IMPLEMENTATION USING VPN AND METRONET NETWORK AT ASTRIDOGROUP INDONESIA*

Agni Isador Harsapranata

AMIK BSI Bekasi  
Jl. Raya Kaliabang No. 8, Perwira, Bekasi Utara  
agniisador@gmail.com

### Abstrak

Tujuan dari penelitian ini adalah untuk membangun jaringan yang menghubungkan kantor pusat dan kantor cabang Astridogroup Indonesia, dengan harapan kinerja dari koneksi jaringan dapat ditingkatkan untuk mendukung tujuan bisnis. Untuk memenuhi kebutuhan tersebut dan kegagalan teknologi komunikasi yang digunakan, dimana teknologi ini menggunakan koneksi yang selalu bisa online dengan harapan kualitas layanan mendekati 100%. Teknologi yang digunakan adalah dengan menggunakan dua jalur koneksi, yang pertama dengan menggunakan serat optik MetroNET, dan yang kedua adalah VPN dengan menggunakan *wifi* internet, sehingga jika salah satu koneksi mati, koneksi lain akan menjadi *backup* secara otomatis.

**Kata Kunci:** VPN, *failover*, mikrotik, kualitas layanan

### Abstract

*The purpose of this research is to build a network that connects the head office and branch offices Astridogroup Indonesia, with the hope that the network connection performance can be improved to support the business objectives. To meet the need for the network connection and to cope with the communication technology failure, the technology suggested allows nearly 100% service quality of online connection. Using two connection line technology, involving optical fiber Metronet and VPN with wifi internet, is expected to provide automatic backup when the other connection drops.*

**Keywords:** VPN, *failover*, microtic, quality of service

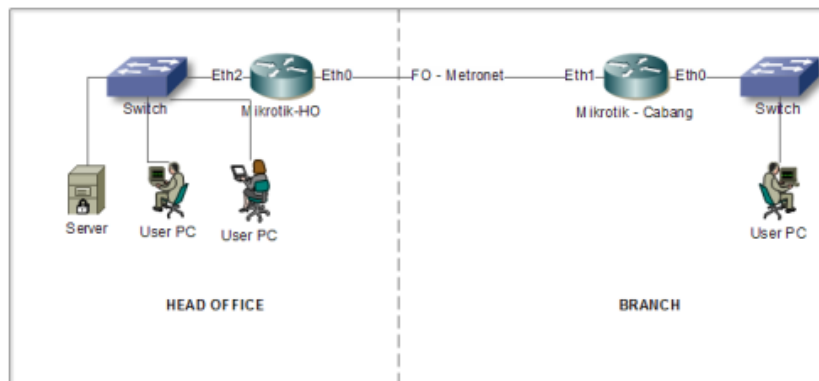
**Tanggal Terima Naskah** : 22 Oktober 2014  
**Tanggal Persetujuan Naskah** : 12 Desember 2014

## 1. PENDAHULUAN

Suatu jaringan komputer yang benar diharapkan dapat menghubungkan dua lokasi yang berbeda untuk dapat saling berkomunikasi dengan lancar dan aman. Untuk saat ini di Astridogroup, koneksi disediakan untuk menghubungkan dari kantor pusat ke kantor cabang, dengan jumlah cabang 20 kantor cabang. Astridogroup yang memanfaatkan jaringan koneksi data dari kantor pusat ke kantor cabang, sangat tergantung terhadap kualitas layanan jaringan tersebut. Seluruh aktivitas yang berhubungan dengan sistem informasi perusahaan, yang dilakukan di kantor cabang, dapat

dilakukan dengan menggunakan koneksi Metronet *Fiber Optic*. Tanpa koneksi tersebut sistem informasi tidak akan dapat dipergunakan. Seluruh sistem informasi ini meliputi aplikasi *e-mail*, aplikasi perusahaan, aplikasi yang berhubungan dengan *supplier*, dan aplikasi perbankan [1].

Untuk koneksi dari kantor pusat ke kantor cabang, selain menggunakan koneksi Metronet *Fiber Optic*, perusahaan juga memanfaatkan teknologi VPN (*Virtual Private Network*). Dengan semakin berkembangnya jaringan publik internet saat ini banyak perusahaan memanfaatkan teknologi VPN tersebut dalam melakukan koneksi dari kantor pusat ke kantor cabang. Dalam hal ini, kedua koneksi tersebut, baik menggunakan Metronet dan VPN, harus diatur sedemikian rupa sehingga setiap kali koneksi utama putus, secara otomatis koneksi VPN akan menggantikannya. Dengan demikian, gangguan yang diakibatkan oleh putusnya koneksi dari kantor pusat ke kantor cabang akan dapat dikurangi. Pergantian koneksi secara otomatis inilah yang sangat diperlukan oleh perusahaan, karena putusnya koneksi dapat terjadi sewaktu-waktu tidak dapat diduga oleh pihak perusahaan. Untuk skema jaringan menggunakan koneksi utama metronet dapat dilihat pada gambar 1 [2].



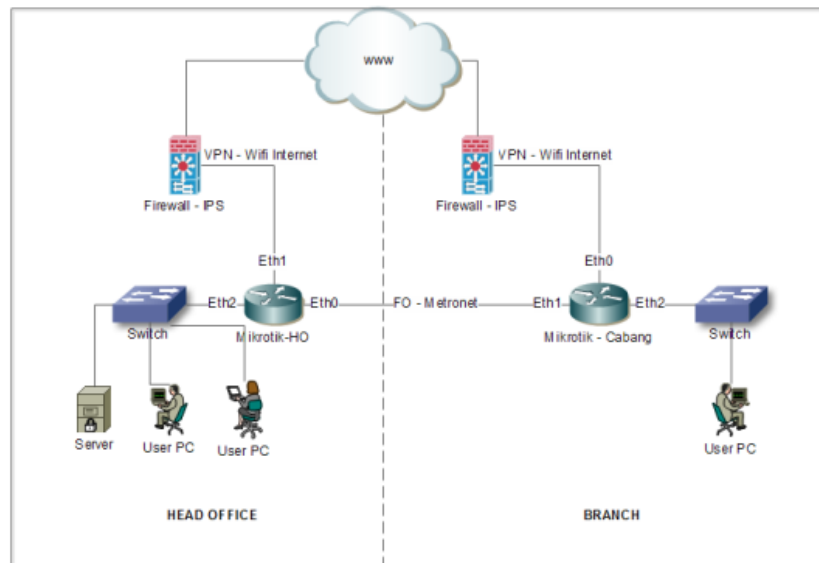
Gambar 1. Skema jaringan metronet *fiber optic*

## 2. PERMASALAHAN

Pada dasarnya komunikasi data dari satu lokasi ke lokasi yang lain memiliki banyak cara, salah satunya adalah menggunakan Metronet *Fiber Optic*. Untuk koneksi menggunakan Metronet *Fiber Optic* permasalahan yang paling sering terjadi adalah putusnya koneksi disebabkan oleh gangguan eksternal. Untuk mengembalikan koneksi Metronet *Fiber Optic* dibutuhkan waktu yang relatif lebih lama. Hal ini disebabkan oleh banyaknya kendala dalam proses penyambungan kabel [3]. Sebagai contoh, untuk proses penyambungan kabel di jalan raya perlu adanya penelusuran kabel dan lain sebagainya.

Untuk itu, diperlukan koneksi alternatif sehingga pada saat koneksi utama putus, koneksi *backup* akan bekerja secara otomatis. Hal ini sangat penting di sisi perusahaan, dikarenakan apabila koneksi dari kantor pusat ke kantor cabang bermasalah, maka semua aplikasi yang harus dikerjakan di cabang akan berhenti. Hal ini mengakibatkan tujuan bisnis dari perusahaan tidak tercapai pada saat itu [4].

Untuk saat ini koneksi Astridogroup dari kantor pusat ke kantor cabang, koneksi utama menggunakan jaringan Metronet *Fiber Optic*. Untuk skema jaringan dapat dilihat pada gambar 1.



Gambar 2. Skema jaringan metronet *fiber optic* dan VPN

Oleh karena itu, perusahaan berusaha untuk mengatasi permasalahan komunikasi data tersebut, sehingga pada saat koneksi utama terputus, koneksi *backup* akan menjalankan fungsinya dengan baik secara otomatis, inilah yang disebut dengan *failover* koneksi.

### 3. KONSEP DASAR

Metode studi pustaka dilakukan untuk menunjang metode wawancara dan observasi yang telah dilakukan. Pengumpulan informasi dilakukan untuk mencari referensi-referensi yang berhubungan dengan penelitian yang dilakukan.

Terdapat beberapa penelitian sebelumnya yang telah dilakukan, yang berkaitan dengan masalah koneksi *failover* ini. Dalam upaya mengembangkan dan menyempurnakan koneksi *failover* perlu dilakukan studi pustaka sebagai salah satu dari penerapan metode penelitian yang akan dilakukan, diantaranya:

1. Penelitian yang dilakukan oleh Dody Agung Wicaksono Wahyudi, dengan judul "Implementasi Virtual Private Network server menggunakan Slackware 13 untuk keamanan komunikasi data (studi kasus: PT Time Excelindo ISP)" [4]. Tahun 2011. Penelitian ini menjelaskan mengenai *Virtual Private Network*, yaitu cara untuk mensimulasikan jaringan pribadi melalui jaringan publik, seperti internet. Disebut "virtual" karena bergantung pada penggunaan *virtual*, yaitu koneksi sementara yang tidak memiliki kehadiran fisik secara nyata, tetapi terdiri dari paket diarahkan melalui variasi mesin di internet secara *ad-hoc*. Koneksi *virtual* yang aman dibuat antara dua mesin, mesin dan jaringan, atau dua jaringan. Penerapan VPN dapat meminimalisir penyadapan dari sisi *client* karena pengguna adalah sisi paling lemah dalam sebuah *security*.
2. Penelitian yang dilakukan oleh Nurul Fadilah Zamzami, dengan judul "Implementasi Load Balancing dan Failover menggunakan Mikrotik router OS berdasarkan multihomed gateway pada warung internet "DIGA" [5]. Tahun 2013. Penelitian ini menjelaskan perancangan dan pengujian yang dilakukan terhadap kinerja *multihomed gateway* berbasis mikrotik dengan menggunakan metoda *load balancing* dan *failover* yang digabungkan. Dapat diambil kesimpulan bahwa Hipotesis penulis tentang kinerja *multihomed gateway* pada teknik penggabungan teknik *load*

*balancing* dan *failover* dapat dilakukan pada mikrotik. Pada pengujian *routing* telah membuktikan bahwa *gateway* kedua ISP telah berhasil dipisahkan berdasarkan kebutuhan *bandwidth* lokal ataupun internasional. Dengan demikian, tujuan penulis untuk memperoleh pemisahan jalur internet antara ISP pertama dan kedua sesuai kebutuhan *client* dan dapat saling mem-*backup* antar ISP telah tercapai.

3. Penelitian yang dilakukan oleh I Made Widhi Wirawan dan Komang Tris Sumarianta, dengan judul “Implementasi Load Balance pada jaringan multihoming menggunakan router dengan metode Round Robin” [6]. Tahun 2011. Pada penelitian ini dijelaskan bahwa jaringan *multihoming* merupakan suatu sistem jaringan yang memiliki jalur keluar lebih dari satu. *Load balance* dengan metode *Round Robin*, yaitu menggunakan kedua *gateway* secara bersamaan dengan membagi beban secara berurutan dan bergiliran. Pada perancangan sistem ini digunakan dua buah modem GSM sebagai koneksi internet. Berdasarkan perancangan sistem yang telah dilakukan dapat disimpulkan bahwa *Load Balance* pada jaringan *Multihoming* menggunakan *Router* dengan metode *Round Robin* merupakan salah satu cara yang dapat digunakan untuk membagi beban *traffic* dari *client* pada beberapa koneksi internet dan bisa sebagai *backup/failover* ketika salah satu koneksi internet mengalami gangguan.
4. Penelitian yang dilakukan oleh Putu Topan Pribadi, dengan judul “Implementasi High-Availability VPN client pada jaringan komputer Fakultas Hukum Universitas Udayana” [7]. Tahun 2013. Pada penelitian ini dijelaskan mengenai ketersediaan data/layanan sangat dibutuhkan, terutama bagi perusahaan-perusahaan yang sangat membutuhkan data-data ataupun layanan yang bersifat sangat penting. Apabila terjadi kerusakan data ataupun layanan, sangat dibutuhkan adanya *server* cadangan. Sesuai dengan dasar teori dari teknologi *High-Availability*, yaitu ilmu untuk menciptakan redundansi dalam setiap sistem dan subsistem untuk memastikan bahwa layanan tetap *up* dan tersedia. Dapat dianalogikan dalam implementasi, bila satu *server* gagal melayani *service* tertentu, maka tugas *server* tersebut otomatis akan dilempar ke *server* lainnya. HA akan diimplementasikan pada layanan *VPN Client* yang bertujuan untuk memastikan koneksi *VPN* tetap hidup, agar *administrator* dapat lebih mudah me-*monitoring* jaringan dari luar.
5. Penelitian yang dilakukan oleh Agus Heriyanto, dengan judul “Analisis dan Implementasi Load Balance dua ISP menggunakan Mikrotik dengan metode Round Robin” [8]. Tahun 2010. Pada penelitian ini dibahas mengenai penggabungan dua ISP menggunakan MikroTik RouterOS dengan *Round Robin* metode Beban *Balance*. Masalah timbul di sini ketika *router* statis memiliki dua atau lebih koneksi yang tersedia ke internet menggunakan ISP yang sama atau berbeda. Jika demikian maka *gateway* dapat digunakan hanya satu saja atau menggunakan *gateway* yang tersisa untuk keperluan *back-up* hanya dalam kasus masalah pada *gateway* pertama. Jadi, untuk bisa menggunakan kedua *gateway* secara bersamaan, sementara memungkinkan mereka untuk satu tujuan *back-up* dalam kasus kegagalan koneksi di gerbang lainnya, maka perlu konsep keseimbangan beban dengan metode *round robin*, yang menggunakan kedua gerbang dan di saat yang sama dengan membagi beban secara berurutan dan bergantian. Hasil dari penelitian ini adalah untuk meningkatkan kapasitas *bandwidth* untuk akses internet karena kedua *gateway* yang tersedia dapat digunakan secara bersamaan. Seiring dengan kegagalan fungsi juga dapat digunakan untuk cadangan tujuan dalam kasus masalah koneksi ke salah satu *gateway*.
6. Penelitian yang dilakukan oleh Aldana Eka Maulana, Bayu Pawitra, Erick Setiawan, Robby Shaleh, dengan judul “Sistem Optimasi pembebanan jaringan dengan koneksi Internet ganda menggunakan Mikrotik” [9]. Tahun 2012. Pada penelitian ini dijelaskan bahwa untuk menunjang kinerja jaringan dengan koneksi Internet lebih dari satu ISP, dibutuhkan sistem yang mampu mengelola jaringan tersebut secara

lebih dinamis. Penelitian ini membahas solusi permasalahan tersebut dengan menerapkan metode *load balancing* dengan kombinasi sistem *failover*. Dengan menggunakan *router MikroTik* sebagai *gateway* untuk jaringan lokal dengan jumlah ISP ganda, koneksi ke Internet yang dijalin oleh *host* pada LAN diolah dengan metode *per-connection classifier* untuk melakukan pembagian beban ke beberapa ISP tersebut, dipadu dengan metode *failover* yang memanfaatkan karakteristik pencarian *nexthop* yang dilakukan oleh *router* dengan *static routing* menjadi sebuah sistem yang dapat memberikan solusi untuk kondisi jaringan tersebut.



Gambar 3. Router mikrotik CRS125-24G-1S-2HnD-IN

Dari enam *Literature Review* yang ada, telah banyak penelitian *failover* dan pembahasan perihal *Virtual Private Network*. Di samping itu, juga terdapat pembahasan mengenai manfaat dari koneksi *failover*. Namun, dapat disimpulkan pula bahwa belum ada penelitian yang secara khusus membahas mengenai perancangan *failover* di jaringan *Wide Area Network*, yang digunakan dalam mengatasi koneksi yang terputus, seperti skema pada gambar 2. Dalam melakukan *failover*, untuk dua koneksi tersebut dilakukan oleh *router mikrotik*.

#### 4. METODE PENELITIAN

Metodologi penelitian yang digunakan meliputi:

- a. Analisis
  1. Melakukan survei terhadap sistem yang sedang berjalan dengan cara wawancara dengan staf dan manajer IT-*Network*, kemudian menganalisis hasil survei tersebut untuk mendapatkan rumusan masalah yang sedang dihadapi oleh perusahaan dan mendapatkan alternatif pemecahan masalah, yang dapat dengan segera dijalankan.
  2. Studi Literatur yang merupakan teknik pengumpulan data atau informasi dengan mempelajari buku yang berisi konsep dan implementasi *fail-over* menggunakan koneksi VPN dan koneksi metronet, menggunakan *router mikrotik* yang digunakan sebagai dasar dari pengembangan penulisan naskah ini.
- b. Perancangan
 

Perancangan *failover* koneksi, mulai dari topologi koneksi VPN dan koneksi metronet *fiber optic*, dengan menggunakan *router mikrotik*, baik dari sisi kantor pusat dan kantor cabang, beserta alat-alat jaringan yang akan digunakan dalam implementasi ini.
- c. Membangun Simulasi Jaringan *failover*

Membangun rancangan *failover* menggunakan *software virtual machine*, *virtual box google*, dimana dengan menggunakan *software* tersebut dapat disimulasikan dengan baik koneksi *failover* antara koneksi VPN dan koneksi metronet *fiber optic*.
- d. Pengujian Simulasi Jaringan
 

Jaringan yang telah disimulasi akan diuji untuk melihat bagaimana kinerjanya dan kemudian mengevaluasinya. Dengan evaluasi ini diharapkan solusi yang didapat, akan segera untuk diimplementasikan di lapangan.

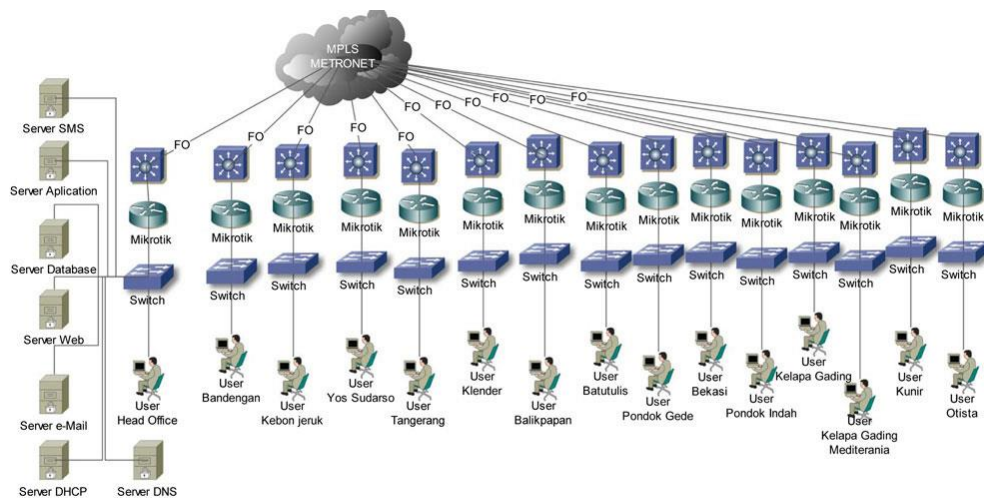
## 5. PEMECAHAN MASALAH

Teknologi *failover* yang akan digunakan dalam menunjang jaringan di Astridogroup ini menggunakan fasilitas yang disediakan oleh *router mikrotik*.



Gambar 4. Topologi metronet

Untuk skema jaringan dapat dilihat di gambar 4 dan belum tersedianya *failover* dapat dilihat di gambar 5.



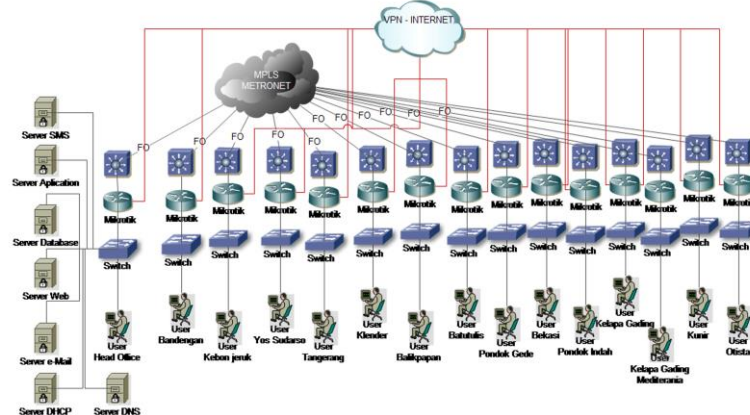
Gambar 5. Arsitektur jaringan astridogroup menggunakan metronet *fiber optic*

Untuk melakukan komunikasi dari dari kantor cabang ke kantor pusat, semua perangkat harus terkoneksi melalui jaringan WAN, dimana untuk IP *network* di setiap cabang adalah sebagai berikut :

- a. *Head Office* : 192.168.1.0/24
- b. Bandengan : 192.168.10.0/24
- c. Kebon Jeruk : 192.168.12.0/24
- d. Yos Sudarso : 192.168.13.0/24
- e. Tangerang : 192.168.14.0/24
- f. Klender : 192.168.15.0/24
- g. Balikpapan : 192.168.16.0/24
- h. Batu tulis : 192.168.17.0/24

- i. Pondok Gede : 192.168.18.0/24
- j. Bekasi : 192.168.19.0/24
- k. Pondok Indah : 192.168.20.0/24
- l. Kelapa Gading : 192.168.21.0/24
- m. Mediterania : 192.168.22.0/24
- n. Kunir : 192.168.23.0/24
- o. Otista : 192.168.24.0/24

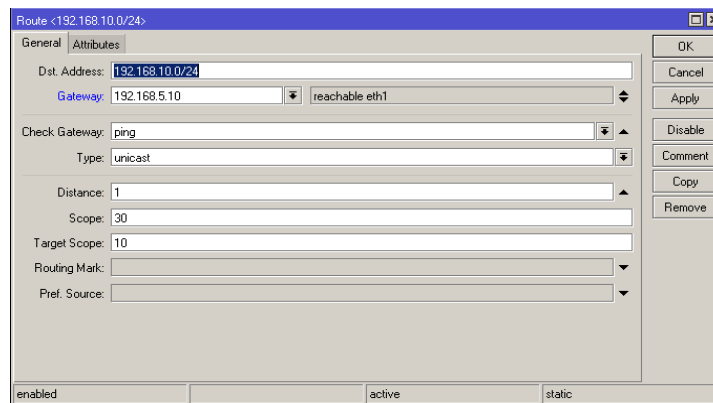
Untuk IP setiap *router*, dimana untuk setiap *router* memiliki 3 *interface*, 1 untuk LAN, 1 untuk koneksi Metronet, 1 untuk koneksi VPN.



Gambar 6. Arsitektur jaringan astridogroup menggunakan metronet *fiber optic* dan VPN

*Bandwidth* yang digunakan untuk *head office* dengan menggunakan koneksi metronet adalah 20 Mbps, sedangkan *bandwidth* di setiap cabang sebesar 1 Mbps. Selanjutnya dengan menggunakan koneksi VPN, *bandwidth* internet yang tersedia di *head office* adalah 10 Mbps, dan *bandwidth* di setiap cabang adalah 1 Mbps. Topologi yang digunakan dalam konfigurasi jaringan ini adalah *star*. Dengan menggunakan topologi tersebut, akan mudah bila ada penambahan segmen jaringan untuk kantor baru. Untuk arsitektur jaringan VPN dan Metronet dapat dilihat di gambar 6.

Dengan adanya penambahan koneksi menggunakan koneksi VPN, maka perlu dilakukan perubahan konfigurasi di sisi *router*, dengan tujuan agar pada saat koneksi utama, yaitu koneksi metronet Metronet *Fiber Optic* bermasalah, secara otomatis koneksi data akan berpindah ke koneksi VPN, dan apabila koneksi utama sudah pulih seperti sediakala, maka koneksi akan berpindah secara otomatis ke koneksi utama.



Gambar 7. Routing link utama menggunakan mikrotik



Untuk konfigurasi di sisi kantor pusat yang harus dilakukan adalah melakukan konfigurasi. Berikut contoh konfigurasi dari salah satu kantor cabang:

Untuk *routing* tujuan Bandengan

```
/ip route
add disabled=no distance=1 dst-address=192.168.10.0/24 gateway=192.168.5.10
scope=30 target-scope=10 check-gateway=ping
add disabled=no distance=4 dst-address=192.168.10.0/24 gateway=192.168.4.10
scope=30 target-scope=10 check-gateway=ping
```

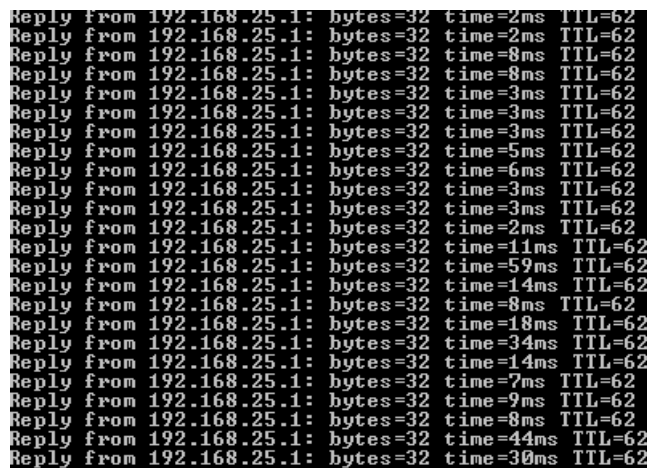
Bila konfigurasi menggunakan *winbox*, yaitu *tools* yang disediakan oleh *mikrotik* untuk melakukan *remote* terhadap router tersebut, dapat dilihat digambar 7.

Untuk *routing* dari cabang ke kantor pusat harus melakukan konfigurasi, berikut salah satu contoh perintah *routing*:

*Routing* di Bandengan ke kantor pusat

```
/ip route
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=192.168.5.1 scope=30
target-scope=10 check-gateway=ping
add disabled=no distance=4 dst-address=0.0.0.0/0
gateway=192.168.4.1 scope=30 target-scope=10 check-gateway=ping
```

Berikut adalah hasil uji perpindahan dari metronet ke VPN dapat dilihat di gambar 8.



```
Reply from 192.168.25.1: bytes=32 time=2ms TTL=62
Reply from 192.168.25.1: bytes=32 time=2ms TTL=62
Reply from 192.168.25.1: bytes=32 time=8ms TTL=62
Reply from 192.168.25.1: bytes=32 time=8ms TTL=62
Reply from 192.168.25.1: bytes=32 time=3ms TTL=62
Reply from 192.168.25.1: bytes=32 time=3ms TTL=62
Reply from 192.168.25.1: bytes=32 time=3ms TTL=62
Reply from 192.168.25.1: bytes=32 time=5ms TTL=62
Reply from 192.168.25.1: bytes=32 time=6ms TTL=62
Reply from 192.168.25.1: bytes=32 time=3ms TTL=62
Reply from 192.168.25.1: bytes=32 time=3ms TTL=62
Reply from 192.168.25.1: bytes=32 time=2ms TTL=62
Reply from 192.168.25.1: bytes=32 time=11ms TTL=62
Reply from 192.168.25.1: bytes=32 time=59ms TTL=62
Reply from 192.168.25.1: bytes=32 time=14ms TTL=62
Reply from 192.168.25.1: bytes=32 time=8ms TTL=62
Reply from 192.168.25.1: bytes=32 time=18ms TTL=62
Reply from 192.168.25.1: bytes=32 time=34ms TTL=62
Reply from 192.168.25.1: bytes=32 time=14ms TTL=62
Reply from 192.168.25.1: bytes=32 time=7ms TTL=62
Reply from 192.168.25.1: bytes=32 time=9ms TTL=62
Reply from 192.168.25.1: bytes=32 time=8ms TTL=62
Reply from 192.168.25.1: bytes=32 time=44ms TTL=62
Reply from 192.168.25.1: bytes=32 time=30ms TTL=62
```

Gambar 8. Hasil uji *ping* dari kantor pusat ke cabang Bekasi

Dapat dilihat pada gambar 8 bahwa *delay time* untuk koneksi menggunakan metronet berkisar 1 digit, sedangkan apabila beralih ke VPN berkisar 2 digit. Waktu transisi saat koneksi metronet putus dan beralih ke VPN hampir tidak membutuhkan waktu yang lama.

## 6. KESIMPULAN

Setelah melakukan analisis, perancangan, dan melakukan simulasi koneksi metronet Metronet *Fiber Optic* dan VPN secara *failover*, maka dapat diambil kesimpulan sebagai berikut:

1. Dengan adanya koneksi *backup*, yaitu VPN (*Virtual Private Network*) sangat membantu, apabila koneksi utama bermasalah. VPN adalah teknologi yang sangat membantu, karena bila ada koneksi internet maka koneksi VPN dapat dijalankan.
2. Dengan menggunakan konfigurasi *failover*, yang dikontrol oleh *mikrotik*, QoS pertukaran data dari kantor pusat ke kantor cabang dan sebaliknya dapat mendekati



100%. Hal ini dikarenakan gangguan terhadap salah satu koneksi dapat di *backup* oleh koneksi yang lain. Perpindahan koneksi dari koneksi utama ke koneksi *backup* tidak memerlukan campur tangan manusia, semua dikerjakan oleh mesin.

## REFERENSI

- [1]. Cisco Systems Inc, 2003, "Cisco Networking Academy Program CCNA 1 and 2 Companion Guide Third Edition", Cisco Press.
- [2]. Cisco Systems Inc, 2001, "Cisco Networking Academy Program Second-Year Companion Guide Second Edition", Cisco Press.
- [3]. Rendra Towidjojo, 2012, "Konsep & Implementasi Routing dengan Router Mikrotik 100% Connected", Jasakom.
- [4]. Dody Agung Wicaksono Wahyudi, 2011, "Implementasi Virtual Private Network server menggunakan Slackware 13 untuk keamanan komunikasi data (studi kasus : PT. Time Excelindo ISP)", Skripsi. STMIK AMIKOM Indonesia.
- [5]. Nurul Fadilah Zamzami, 2013, "Implementasi Load Balancing dan Failover menggunakan Mikrotik router OS berdasarkan multihomed gateway pada warung internet "DIGA" ", Skripsi. UDINUS Indonesia.
- [6]. I Made Widhi Wirawan, Komang Tris Sumarianta, 2011, "Implementasi Load Balance pada jaringan multihoming menggunakan router dengan metode Round Robin", Jurnal Ilmu Komputer - Volume 4 - No 1, Universitas Udayana.
- [7]. Putu Topan Pribadi, 2013, "Implementasi High-Availability VPN client pada jaringan komputer Fakultas Hukum Universitas Udayana", Jurnal Ilmu Komputer - Volume 6 - No 1, Universitas Udayana.
- [8]. Agus Heriyanto, 2010, "Analisis dan Implementasi Load Balance dua ISP menggunakan Mikrotik dengan metode Round Robin", Skripsi. STMIK AMIKOM: Indonesia.
- [9]. Aldana Eka Maulana, Bayu Pawitra, Erick Setiawan, Robby Shaleh, 2012, "Sistem Optimasi pembebanan jaringan dengan koneksi Internet ganda menggunakan Mikrotik", Thesis. Binus Indonesia.