

## IMPLEMENTASI FAILOVER MENGGUNAKAN JARINGAN VPN DAN METRONET PADA ASTRIDOGROUP INDONESIA

Agni Isador Harsapranata<sup>1</sup>

*e-mail : agniisador@gmail.com*

Diterima : 28 Oktober 2014 / Disetujui : 10 Desember 2014

### ABSTRACT

*The purpose of this research is to build a network that connects the head office and branch offices Astridogroup Indonesia, with the hope of the entire performance can be improved connections to support business objectives. To meet these needs and the failures of communication technology that was used, in which the technology is to use a connection that can always be online in the hope of quality of service close to 100%. The technology used is to use two connection lines, the first is to use optical fiber Metronet, and the second VPN using wifi internet, so that if one connection dies , the another connection would be a backup, to set both the connection failover using mikrotik router.*

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

### ABSTRAK

Tujuan dari penelitian ini adalah untuk membangun jaringan yang menghubungkan kantor pusat dan kantor cabang Astridogroup Indonesia, dengan harapan seluruh kinerja koneksi dapat ditingkatkan untuk mendukung tujuan bisnis perusahaan. Untuk memenuhi kebutuhan tersebut dan mengatasi kegagalan teknologi komunikasi yang digunakan, di mana teknologi ini menggunakan koneksi yang dapat selalu online dengan harapan quality of service mendekati 100%. Teknologi yang digunakan adalah dengan menggunakan dua jalur koneksi, yang pertama adalah menggunakan Metronet Fiber Optik , dan yang kedua VPN dengan menggunakan internet wifi, sehingga apabila salah satu koneksi mati koneksi yang lain akan menjadi backup, untuk mengatur kedua failover koneksi tersebut menggunakan router mikrotik.

Kata Kunci : VPN, failover, mikrotik, quality of service

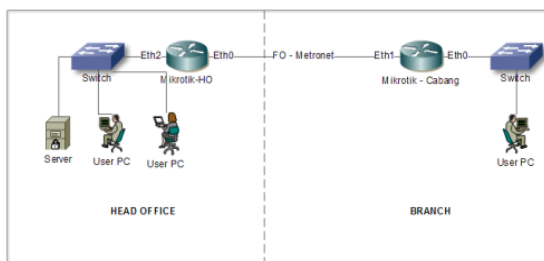
### PENDAHULUAN

Suatu jaringan yang benar diharapkan dapat menghubungkan dua lokasi yang berbeda untuk dapat saling berkomunikasi dengan lancar dan aman. Untuk di Astridogroup, koneksi disediakan untuk menghubungkan dari kantor pusat ke kantor cabang, dengan jumlah cabang 30 kantor cabang. Astridogroup yang memanfaatkan jaringan koneksi data dari kantor pusat ke ke kantor, 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 Optik, 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.

Untuk koneksi dari kantor pusat ke kantor cabang, selain menggunakan koneksi

Metronet Fiber Optik, perusahaan juga memanfaatkan teknologi VPN. Dengan semakin berkembangnya jaringan publik internet saat ini banyak perusahaan memanfaatkan teknologi VPN dalam melakukan koneksi dari kantor pusat ke kantor cabang. Dengan menggunakan VPN, biaya yang dikeluarkan relatif lebih murah dibandingkan menggunakan koneksi lease line, dimana koneksi lease line adalah koneksi *point to point*, sedangkan VPN dengan menggunakan jaringan internet dimana jaringan public yang setiap perusahaan dapat memanfaatkan koneksi tersebut dan digunakan untuk melakukan koneksi *private* yang terpisah dari koneksi publik internet.



Gambar 1. Skema Jaringan Metronet Fiber Optik

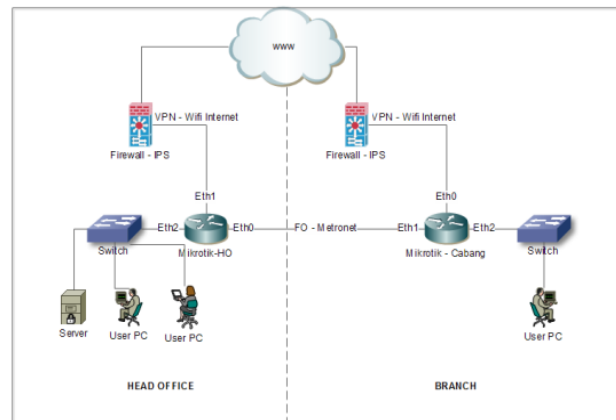
## PERMASALAHAN

Pada dasarnya komunikasi data dari satu lokasi ke lokasi yang lain memiliki banyak cara, salah satunya adalah menggunakan Metronet Fiber Optik. Untuk koneksi menggunakan Metronet Fiber Optik permasalahan yang paling sering terjadi adalah putusnya koneksi disebabkan oleh gangguan eksternal. Untuk mengembalikan koneksi Metronet Fiber Optik dibutuhkan waktu yang relatif lebih lama disebabkan oleh banyaknya kendala dalam proses penyambungan kabel. Sebagai contohnya untuk proses penyambungan kabel di jalan raya perlu adanya penelusuran kabel, untuk masalah di suatu area industri, dibutuhkan

proses perijinan untuk masuk ke area industri, dan lain sebagainya.

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

Untuk saat ini koneksi Astridogroup dari kantor pusat ke kantor cabang, koneksi utama menggunakan jaringan Metronet Fiber Optik, untuk skema jaringan dapat dilihat di gambar 1.



Gambar 2. Skema Jaringan Metronet Fiber Optik 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.

## LITERATUR REVIEW

Metode study pustaka dilakukan untuk menunjang metode wawancara dan observasi yang telah dilakukan. Pengumpulan informasi yang dibutuhkan dalam mencari referensi-referensi yang

berhubungan dengan penelitian yang dilakukan.

Ada beberapa penelitian sebelumnya yang telah dilakukan yang berkaitan dengan masalah koneksi failover ini. Dalam upaya mengembangkan dan menyempurnakan koneksi failover perlu dilakukan studi pustaka (literature review) sebagai salah satu dari penerapan metode penelitian yang akan dilakukan. Diantaranya yaitu:

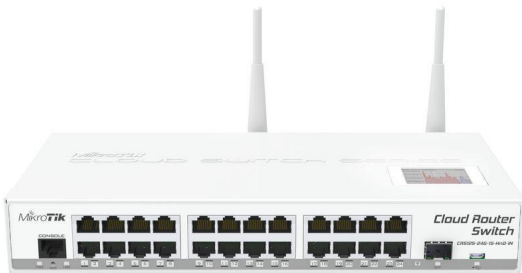
1. Penelitian ini dilakukan oleh Dody Agung Wicaksono Wahyudi, dengan judul "Implementasi Virtual Private Network server menggunakan Slackware 13 untuk keamanan komunikasi data (studi kasus : PT. Time Excelindo ISP)". Tahun 2011. Penelitian ini menjelaskan mengenai Virtual Private Network adalah cara untuk mensimulasikan jaringan pribadi melalui jaringan publik, seperti internet. Disebut "virtual" karena bergantung pada penggunaan virtual yaitu koneksi, koneksi sementara yang tidak memiliki kehadiran fisik secara nyata, tetap terdiri dari paket diarahkan melalui variasi mesin di internet secara ad-hoc. Koneksi virtual yang aman yang dibuat antara dua mesin, mesin dan jaringan, atau dua jaringan. Penerapan VPN bisa meminimalisir penyadapan dari sisi klien karena pengguna adalah sisi paling lemah dalam sebuah sekuriti.
2. Penelitian ini dilakukan oleh Nurul Fadilah Zamzami, dengan judul "Implementasi Load Balancing dan Failover menggunakan Mikrotik router OS berdasarkan multihomed gateway pada warung internet "DIGA". 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 maka 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 antasa isp pertama dan kedua sesuai kebutuhan client dan dapat saling mem-backup antar isp telah tercapai.

3. Penelitian ini dilakukan oleh I Made Widhi Wirawan dan Komang Tris Sumarianta, dengan judul "Implementasi Load Balance pada jaringan multihoming menggunakan router dengan metode Round Robin". Tahun 2011. Pada penelitian ini menjelaskan 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 ini dilakukan oleh Putu Topan Pribadi, dengan judul “Implementasi High-Availability VPN client pada jaringan komputer Fakultas Hukum Universitas Udayana”. 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. Sehingga 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 ini dilakukan oleh Agus Heriyanto, dengan judul “Analisis dan Implementasi Load Balance dua ISP menggunakan Mikrotik dengan metode Round Robin”. Tahun 2010. Pada penelitian ini dibahas mengenai penggabungan dua ISP menggunakan MikroTik RouterOS dengan Round Robin metode Beban Balance. Masalah timbul di sini adalah 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 ini dilakukan oleh Aldana Eka Maulana, Bayu Pawitra, Erick Setiawan, Robby Shaleh, dengan judul “Sistem Optimasi pembebanan jaringan dengan koneksi Internet ganda menggunakan Mikrotik”. Tahun 2012. Pada penelitian ini dijelaskan untuk menunjang kinerja jaringan dengan koneksi Internet lebih dari satu ISP, dibutuhkan sistem yang mampu mengelola jaringan tersebut secara lebih dinamis. Seperti manajemen koneksi yang dapat mengelola traffic pada jalur ISP secara efisien dan kemampuan untuk menanggulangi masalah yang umum terjadi secara efektif tanpa adanya tindak lanjut secara langsung dari pengelola jaringan. 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 pembahasannya perihal Virtual Private Network. Di samping itu juga ada pembahasan mengenai manfaat dari koneksi failover. Namun dapat disimpulkan pula bahwa belum ada peneliti yang secara khusus membahas mengenai perancangan failover di jaringan Wide Area Network, yang digunakan dalam mengatasi koneksi yang terputus, seperti skema di gambar 2. Dalam melakukan failover, untuk 2 koneksi tersebut dilakukan oleh router mikrotik, seperti terlihat di gambar 3.

## METODE PENELITIAN

Metodologi 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 di jalankan.
2. Studi Literatur yang merupakan teknik pengumpulan data atau informasi dengan mempelajari buku buku yang berisi konsep dan implementasi fail-over menggunakan koneksi VPN dan koneksi metronet, menggunakan router mikrotik yang digunakan sebagai dasar dari pengembangan penulisan artikel ini.

### b. Perancangan

Perancangan failover koneksi, mulai dari topologi koneksi VPN dan koneksi metronet fiber optik, 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

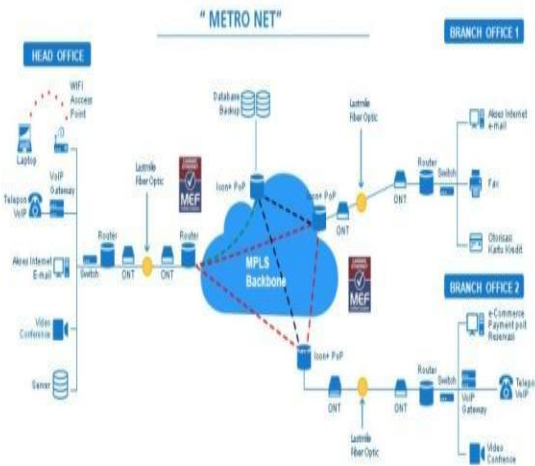
Membangun rancangan failover menggunakan software *virtual machine*, *virtual box google*, dimana dengan menggunakan software tersebut dapat disimulasikan dengan baik koneksi failover antara koneksi VPN dan koneksi metronet fiber optik.

### 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 dilapangan.

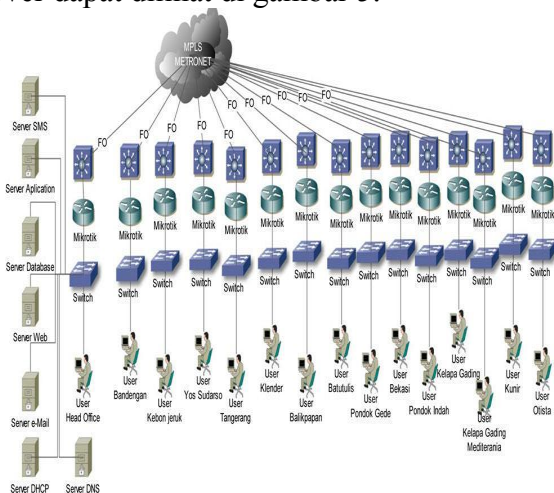
**PEMECAHAN MASALAH**

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



Gambar 4. Topologi Metronet

Dimana untuk arsitektur jaringan pada saat menggunakan Metronet Fiber Optik, dimana untuk skema jaringan dapat dilihat di gambar 4 dan belum tersediaanya failover dapat dilihat di gambar 5.



Gambar 5. Arsitektur Jaringan Astrido Group menggunakan Metronet Fiber Optik

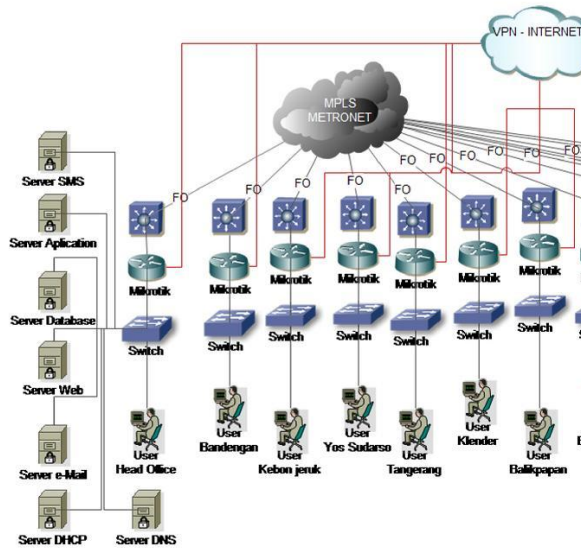
Untuk melakukan komunikasi dari dari kantor cabang ke kantor pusat, semua perangkat harus terkoneksi melalui jaringan

WAN, dimana untuk ip network di setiap cabang adalah sebagai berikut :

- Head Office : 192.168.1.0/24
- Bandengan : 192.168.10.0/24
- Kebon Jeruk : 192.168.12.0/24
- Yos Sudarso : 192.168.13.0/24
- Tangerang : 192.168.14.0/24
- Klender : 192.168.15.0/24
- Balikpapan : 192.168.16.0/24
- Batu tulis : 192.168.17.0/24
- Pondok Gede : 192.168.18.0/24
- Bekasi : 192.168.19.0/24
- Pondok Indah : 192.168.20.0/24
- Kelapa Gading : 192.168.21.0/24
- Mediterrania : 192.168.22.0/24
- Kunir : 192.168.23.0/24
- Otista : 192.168.24.0/24

Dan untuk ip setiap router, dimana untuk setiap router memiliki 3 interface, 1 untuk LAN, 1 untuk koneksi Metronet, 1 untuk koneksi VPN, adalah sebagai berikut :

- Head Office
- eth0 : 192.168.1.1/24
- eth1 : 192.168.5.1/27
- eth2 : 192.168.4.1/27



Gambar 6. Arsitektur Jaringan Astrido Group menggunakan Metronet Fiber Optik dan VPN Bandengan

eth0 : 192.168.10.1/24  
 eth1 : 192.168.5.10/27  
 eth2 : 192.168.4.10/27

Kebon Jeruk

eth0 : 192.168.12.1/24  
 eth1 : 192.168.5.12/27  
 eth2 : 192.168.4.12/27

Yos Sudarso

eth0 : 192.168.13.1/24  
 eth1 : 192.168.5.13/27  
 eth2 : 192.168.4.13/27

Tangerang

eth0 : 192.168.14.1/24  
 eth1 : 192.168.5.14/27  
 eth2 : 192.168.4.14/27

Klender

eth0 : 192.168.15.1/24  
 eth1 : 192.168.5.15/27  
 eth2 : 192.168.4.15/27

Balikpapan

eth0 : 192.168.16.1/24  
 eth1 : 192.168.5.16/27  
 eth2 : 192.168.4.16/27

Batu tulis

eth0 : 192.168.17.1/24  
 eth1 : 192.168.5.17/27  
 eth2 : 192.168.4.17/27

Pondok Gede

eth0 : 192.168.18.1/24  
 eth1 : 192.168.5.18/27  
 eth2 : 192.168.4.18/27

Bekasi

eth0 : 192.168.19.1/24  
 eth1 : 192.168.5.19/27  
 eth2 : 192.168.4.19/27

Pondok Indah

eth0 : 192.168.20.1/24  
 eth1 : 192.168.5.20/27  
 eth2 : 192.168.4.20/27

Kelapa Gading

eth0 : 192.168.21.1/24  
 eth1 : 192.168.5.21/27  
 eth2 : 192.168.4.21/27

Mediterrania

eth0 : 192.168.22.1/24  
 eth1 : 192.168.5.22/27  
 eth2 : 192.168.4.22/27

Kunir

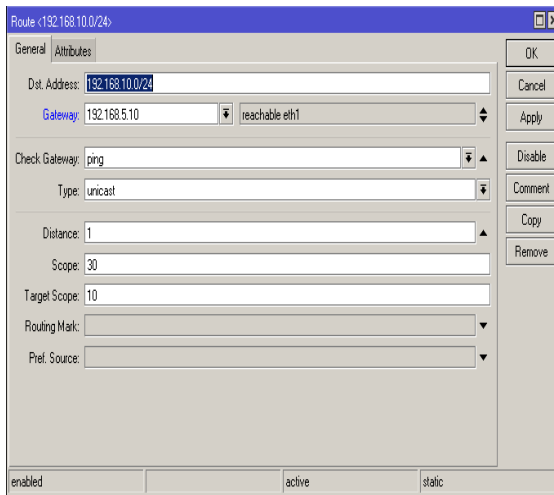
eth0 : 192.168.23.1/24  
 eth1 : 192.168.5.23/27  
 eth2 : 192.168.4.23/27

Otista

eth0 : 192.168.24.1/24  
 eth1 : 192.168.5.24/27  
 eth2 : 192.168.4.24/27

Bandwidth yang digunakan untuk head office dengan menggunakan koneksi metronet adalah 20 Mbps, sedangkan bandwidth di setiap cabang sebesar 1 Mbps, kemudian 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 akan 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 disisi router, dengan tujuan supaya pada saat koneksi utama, yaitu koneksi metronet Metronet Fiber Optik bermasalah, secara otomatis, koneksi data akan berpindah ke koneksi VPN, dan apabila koneksi utama sudah pulih seperti sedia kala, maka koneksi akan berpindah secara otomatis ke koneksi utama.



*Gambar 7. Routing Link Utama Menggunakan Mikrotik*

Untuk konfigurasi disisi kantor pusat yang harus dilakukan adalah melakukan konfigurasi sebagai berikut:

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
```

Untuk routing tujuan Kebon Jeruk

```
/ip route
add disabled=no distance=1 dst-address=192.168.12.0/24
gateway=192.168.5.12 scope=30 target-scope=10 check-gateway=ping
```

```
add disabled=no distance=4 dst-address=192.168.12.0/24
gateway=192.168.4.12 scope=30 target-scope=10 check-gateway=ping
Untuk routing tujuan Yos Sudarso
/ip route
```

```
add disabled=no distance=1 dst-address=192.168.13.0/24
gateway=192.168.5.13 scope=30 target-scope=10 check-gateway=ping
add disabled=no distance=4 dst-address=192.168.13.0/24
gateway=192.168.4.13 scope=30 target-scope=10 check-gateway=ping
```

Untuk routing tujuan Tangerang

```
/ip route
add disabled=no distance=1 dst-address=192.168.14.0/24
gateway=192.168.5.14 scope=30 target-scope=10 check-gateway=ping
```

```
add disabled=no distance=4 dst-address=192.168.14.0/24
gateway=192.168.4.14 scope=30 target-scope=10 check-gateway=ping
```

Untuk routing tujuan Klender

```
/ip route
add disabled=no distance=1 dst-address=192.168.15.0/24
gateway=192.168.5.15 scope=30 target-scope=10 check-gateway=ping
```

```
add disabled=no distance=4 dst-address=192.168.15.0/24
gateway=192.168.4.15 scope=30 target-scope=10 check-gateway=ping
```

Untuk routing tujuan Balikpapan

```
/ip route
add disabled=no distance=1 dst-address=192.168.16.0/24
gateway=192.168.5.16 scope=30 target-scope=10 check-gateway=ping
```

```
add disabled=no distance=4 dst-address=192.168.16.0/24
gateway=192.168.4.16 scope=30 target-scope=10 check-gateway=ping
```

Untuk routing tujuan Batu tulis

```
/ip route
```

```

add disabled=no distance=1 dst-
address=192.168.17.0/24
gateway=192.168.5.17 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.17.0/24
gateway=192.168.4.17 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Pondok Gede
/ip route
add disabled=no distance=1 dst-
address=192.168.18.0/24
gateway=192.168.5.18 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.18.0/24
gateway=192.168.4.18 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Bekasi
/ip route
add disabled=no distance=1 dst-
address=192.168.19.0/24
gateway=192.168.5.19 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.19.0/24
gateway=192.168.4.19 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Pondok Indah
/ip route
add disabled=no distance=1 dst-
address=192.168.20.0/24
gateway=192.168.5.20 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.20.0/24
gateway=192.168.4.20 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Kelapa Gading
/ip route
add disabled=no distance=1 dst-
address=192.168.21.0/24
gateway=192.168.5.21 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.21.0/24

```

```

gateway=192.168.4.21 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Mediterania
/ip route
add disabled=no distance=1 dst-
address=192.168.22.0/24
gateway=192.168.5.22 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.22.0/24
gateway=192.168.4.22 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Kunir
/ip route
add disabled=no distance=1 dst-
address=192.168.23.0/24
gateway=192.168.5.23 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.23.0/24
gateway=192.168.4.23 scope=30 target-
scope=10 check-gateway=ping
  Untuk routing tujuan Otista
/ip route
add disabled=no distance=1 dst-
address=192.168.24.0/24
gateway=192.168.5.24 scope=30 target-
scope=10 check-gateway=ping
add disabled=no distance=4 dst-
address=192.168.24.0/24
gateway=192.168.4.24 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 sebagai berikut:

```

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
```

Routing di Kebon Jeruk 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
```

Routing di Yos Sudarso 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
```

Routing di Tangerang 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
```

Routing di Klender 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
```

Routing di Balikpapan 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
```

Routing di Batu tulis 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
```

Routing di Pondok Gede 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
```

Routing di Bekasi 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
```

Routing di Pondok Indah 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
```

Routing di Kelapa Gading 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
```

routing di Mediterania 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
```

Routing di Kunir 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
```

Routing di Otista 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 4.4.

```
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=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 di gambar 8 delay time untuk koneksi menggunakan metronet berkisar 1 digit, sedangkan apabila beralih ke VPN berkisar 2 digit. Dan waktu transisi saat koneksi metronet putus dan beralih ke VPN hampir tidak membutuhkan waktu yang lama.

## KESIMPULAN

Setelah melakukan analisa, perancangan, dan melakukan simulasi koneksi metronet Metronet Fiber Optik dan VPN, maka penulis dapat mengambil kesimpulan sebagai berikut :

Dari analisa kondisi jaringan saat penulis melakukan penelitian di Astridogroup didapatkan bahwa belum ada backup koneksi dari kantor pusat ke kantor cabang. Sehingga akan mengakibatkan gangguan koneksi apabila koneksi utama metronet bermasalah. Dengan adanya koneksi alternatif 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.

Dengan menggunakan konfigurasi *failover*, yang dikontrol oleh mikrotik, qos pertukaran data dari kantor pusat ke kantor cabang dan

sebaliknya dapat mendekati 100%, dikarenakan gangguan terhadap salah satu koneksi dapat di backup oleh koneksi yang lain.

#### DAFTAR PUSTAKA

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.