p-ISSN 2477-3506
e-ISSN 2549-1938

PENERAPAN FAILOVER NETWORK MENGGUNAKAN JARINGAN VPN DAN JARINGAN WIRELESS POINT-TO-POINT PADA DISTANCE BUILDING DI PT. TITIPAN KILAT RIAU

Afdhil Hafid[1], Harun Mukhtar[2], Dani Harlian[3]

[1]Fakultas Sains dan Teknologi, Universitas Islam Negeri Imam Bonjol, Padang
[2,3]Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau, Pekanbaru
Email: [1]afdhilhafid@uinib.ac.id, [2]harunmukhtar@umri.ac.id, [3]dani.harlian@student.umri.ac.id

Abstrak

Abstrak-- Penelitian ini dimaksudkan untuk menerapkan jaringan yang dapat menghubungkan antara kantor cabang dengan kantor pusat pada sebuah perusahaan. Hal ini dilakukan dalam rangka menciptakan seluruh kinerja yang terkoneksi pada sebuah jaringan perusahaan dapat ditingkatkan dan berjalan dengan baik, sehingga mampu mendukung proses bisnis perusahaan. Pada tahapan pemenuhan kebutuhan perusahaan dan dalam upaya mengatasi permasalahan pada jaringan yang digunakan, dengan teknologi daring, menitikberatkan terhadap capaian kualitas layanan atau *quality of services* (QoS) mendekati 100%. Teknologi yang diterapkan menggunakan dua jalur komunikasi, jalur koneksi pertama merupakan *wireless point-to-point* dan jalur koneksi kedua menerapkan Virtual Private Network (VPN) dengan pemanfaatan internet. Penanganan *failover* pada kedua koneksi komunikasi jaringan digunakan router mikrotik. Hal ini memungkinkan apabila salah satu koneksi terputus / mati maka jalur koneksi lainnya akan secara otomatis menjadi jalur cadangan. Pada simulasi *failover network* ini menunjukkan hasil yang cukup memuaskan terlihat dari kinerja perpindahan jaringan komunikasi dengan tidak membebani *traffic*. Penerapan metode ini juga dapat beroperasi tanpa melibatkan manusia. Selain itu dari hasil pengukuran jeda waktu yang dibutuhkan pada perpindahan jalur koneksi memiliki nilai rata-rata delay tidak lebih dari 4.97 detik.

Kata Kunci: *Failover, Mikrotik, VPN , Wireless Point-to-Point*

Abstract

Abstrak-- This research is intended to build a network that that can connect branch offices with main office buildings in a company. This is done in order to create all performance connected to a company network that can improve and run well, so as to be able to support the company's business processes. At the stage of meeting company needs and in an effort to overcome problems in the network used technology that can always be online with the expectation of quality of services (QoS) approaching 100%.. The technology applied uses two communication lines, the first connection line is point-to-point wireless and the second connection line applies a Virtual Private Network (VPN) with the use of the internet. Handles failover on both network communication connections used by the mikrotik router. This allows if one connection is lost, the other connection line will automatically become a backup line. In this failed network simulation, it shows satisfactory results, as can be seen from the communication performance that runs without feeling tired of traffic. The application of this method can also operate without involving humans. In addition, the results of the measurement of the time lag required for switching connection lines have an average delay value of not more than 4.97 seconds.

Keywords: *Failover, Mikrotik, VPN, Wireless Point-to-Point*

I. PENDAHULUAN

Perkembangan teknologi komunikasi dan informasi memiliki dampak yang besar dalam berbagai aspek dalam kehidupan, diantaranya banyak keuntungan yang kita dapat dan implementasikan. Saat ini peran teknologi mampu memudahkan terutama dalam penyampaian sebuah informasi (Pribadi, 2013). Pada pengaplikasiannya, sebuah jaringan diharapkan dapat menghubungkan beberapa lokasi yang berbeda secara jarak dan tempat untuk dapat saling berkomunikasi secara aman dan lancar, yaitu dengan pemanfaatan VPN (Harsapranata, 2014; Triyono, 2014; Swapna, 2017). Saat ini banyak perusahaan diantaranya PT. Titipan Kilat Riau menerapkan teknologi Virtual Private Network (VPN) untuk menghubungkan jalur komunikasi antara kantor cabang dengan kantor pusat. Koneksi VPN menggunakan jaringan internet dan VPN mampu membuat link virtual yang aman antara bangunan yang berbeda melalui jaringan *public* internet dan memungkinkan pengguna untuk dapat terhubung ke jaringan secara *private* (Varianto, 2015; Harun Mukhtar, dkk, 2017).

Pada dasarnya untuk menghubungkan suatu lokasi dengan lokasi yang lain memiliki banyak cara diantaranya koneksi VPN dan koneksi Wireless Point-to-Point. Koneksi jaringan secara Wireless Point-to-Point (P2P) merupakan aplikasi komunikasi wireless antara dua titik, pada saat sebuah host hanya terhubung dengan satu client (Oba, 2016). Wireless Point-to-Point (P2P) memanfaatkan dua buah perangkat Radio dan Antena Directional (Grid, Sectoral, Yagi, dsb), ketika satu perangkat berfungsi menjadi pengirim (*transmitter*) dan yang lainnya sebagai penerima (*receiver*) (Palaha, 2014). Prinsip *wireless* dengan *wired* pada dasarnya sama, hanya saja medium yang dilaluinya berbeda (Kadir, 2015).

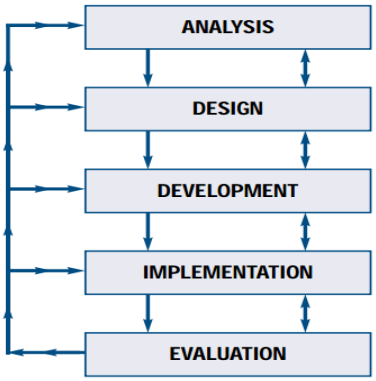
PT. Titipan Kilat Riau merupakan perusahaan yang bergerak pada bidang jasa pengiriman dalam melayani kebutuhan masyarakat serta memiliki layanan jaringan yang saling terhubung antar kantor cabang. PT. Titipan Kilat Riau menggunakan jaringan komunikasi data antara kantor cabang dengan kantor pusat amat bergantung terhadap kualitas dan layanan pada jaringan itu. Setiap pekerjaan yang terkait dengan sistem informasi pada perusahan yang dikerjakan pada kantor cabang saat ini, menmakai koneksi internet VPN (Virtual Private Network) sebagai satu satunya jalur koneksi ke kantor pusat. Tanpa menggunakan koneksi tersebut mengakibatkan sistem informasi saat ini tidak mampu berfungsi dengan baik. Sistem informasi ini terdiri dari aplikasi penjualan dan aplikasi operasional. Pada koneksi jaringan VPN, proses transfer file antar-*site* akan mengacu pada bandwidth terkecil antara kedua *site* sehingga kebutuhan akan komunikasi yang semakin tinggi dari aktifitas perusahaan menuntut koneksi yang lebih cepat dan lebih baik.

Pada jalur komunikasi menggunakan VPN kendala yang paling sering muncul ialah terputusnya koneksi internet yang dipengaruhi oleh gangguan eksternal seperti kerusakan pada modem maupun gangguan cuaca. Upaya mengembalikan koneksi internet seringkali membutuhkan waktu yang cenderung lebih lama disebabkan banyaknya permasalahan pada proses perbaikan dan tidak adanya koneksi alternatif saat koneksi VPN terputus, mengakibatnya proses operasional pada perusahaan mengalami hambatan. Hal ini mengakibatkan data dan status kiriman gagal diperbaharui sehingga harus diproses secara manual.

Pada berbagai permasalahan sistem jaringan komputer diperlukan konfigurasi jaringan dengan pemanfaatan komponen-komponen pendukung yang sesuai (Sopandi, 2008; Sukmaaji & Rianto, 2008). Berdasarkan permasalahan penelitian pada PT. Titipan Kilat Riau maka diperlukan jalur koneksi cadangan agar layanan dapat terus berlangsung meskipun jalur koneksi utama terputus dengan berbagai sebab. Salah satu konfigurasi koneksi *backup* yang dapat dilakukan secara otomatis dengan menggunakan konfigurasi *failover*, yang dapat dikontrol dengan pemanfaatan Mikrotik RouterOS (Zamzami, 2013). Tujuan dari *failover* adalah untuk membantu memastikan akses klien ke sumber daya di server tetap terjaga ketika terjadi kegagalan fungsi perangkat lunak di server atau kegagalan akses ke server. (Purnomo, 2013). QoS pertukaran data dari kantor cabang ke kantor pusat dan sebaliknya diharapkan dapat ditingkatkan secara maksimal. Teknologi *Quality of Service* (QoS) memungkinkan administrator jaringan untuk mengelola dampak dari kemacetan pada aliran paket dari berbagai layanan dengan tujuan memaksimalkan penggunaan sumber daya jaringan (Iskandar, 2014). Penting bagi perusahaan untuk menjaga koneksi antara kantor cabang dan kantor pusat agar tetap terhubung, karena adanya gangguan pada salah satu koneksi dapat diatasi dengan backup koneksi lain. Hal ini krusial karena bila koneksi antara kantor cabang dan kantor pusat terganggu, transfer data antar server akan terhenti, menghambat aktivitas operasional kantor cabang, dan menghambat pencapaian tujuan bisnis perusahaan.

II. METODE

Metode ADDIE merupakan sebuah kerangka yang biasa digunakan oleh perancang dan pengembang jaringan yang terdiri dari lima fase yaitu, *Analysis*, *Design*, *Development*, *Implementation*, dan *Evaluation* seperti yang digambarkan pada diagram berikut :

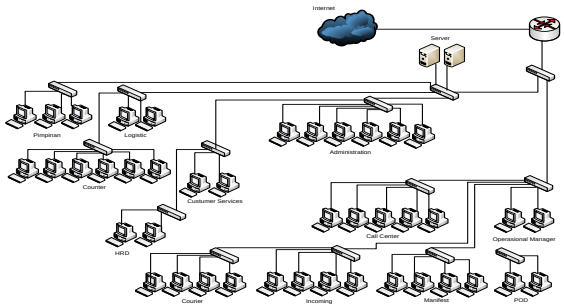


Gambar 1. *Metode* ADDIE Model

III. HASIL DAN PEMBAHASAN

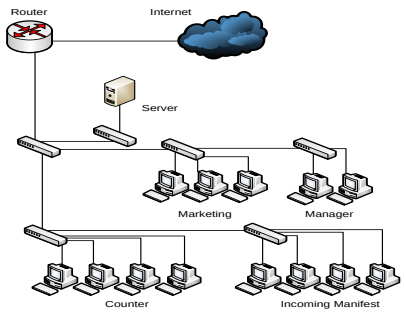
1. Analisis (*Analysis)*

Kantor pusat yang berlokasi di Jl. Rambutan merupakan kantor utama yang sekaligus menjadi pusat seluruh aktifitas operasional dimana seluruh paket masuk diproses terlebih dahulu di kantor pusat yang selanjutnya diteruskan ke kantor cabang. Pada kantor pusat terdapat Server sistem informasi yang meliputi aplikasi penjualan dan aplikasi operasional dan juga terdapat server sms *gateway* yang terhubung ke jaringan komputer dan pada kantor pusat memiliki akses internet dengan besar *bandwidth dedicated* 3Mbps dan memiliki *ip public static*.



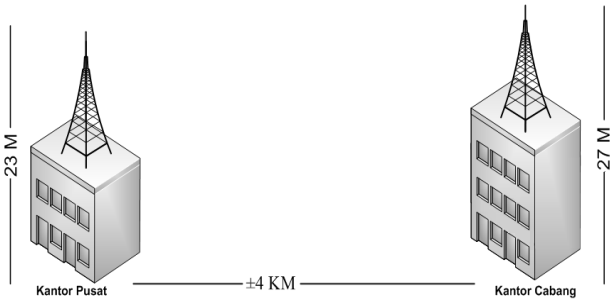
Gambar 2. *Network Architecture* Kantor Pusat

Kantor cabang yang berlokasi di Jl. HR. Subrantas panam merupakan kantor marketing utama sekaligus melayani pengiriman paket. Dalam aktifitas operasional seluruhnya menggunakan sistem informasi dengan data yang saling terkoneksi antara kantor cabang dan kantor pusat melalui internet. Pada kantor cabang memiliki akses internet dengan besar *bandwidth* upto 1Mbps.



Gambar 3. *Network Architecture* Kantor Cabang

Adapun jarak antara kantor pusat ke kantor cabang ±4km dengan ketinggian bangunan kantor pusat ditambah dengan ketinggian tower adalah 23m dan ketinggian bangunan kantor cabang ditambah tower adalah 27m.



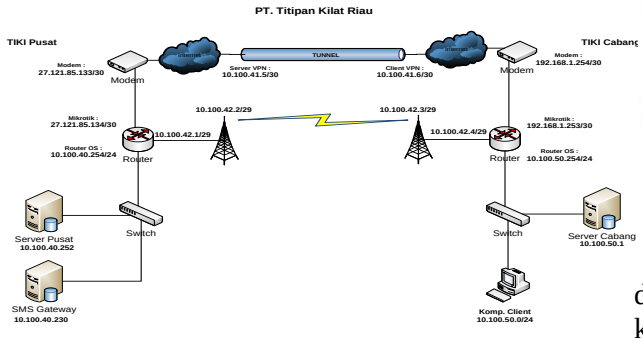
Gambar 4. Kondisi fisik dilapangan

Berdasarkan data diatas dapat diambil kesimpulan yaitu dalam proses implementasi *wireless point-to-point* sebagai jalur utama koneksi jaringan *failover* membutuhkan sebuah alat perangkat jaringan komputer yang dapat menghubungkan kantor cabang dan kantor pusat secara *wireless*. Pada koneksi VPN, transfer file antar site akan mengikuti *bandwidth* terkecil dari kedua site maka berdasarkan data diatas koneksi VPN sebagai jalur backup dengan VPN server berada pada sisi kantor pusat yang memiliki *ip public static*.

2. Desain (*Design*)

Pada tahapan desain ini digambarkan mengenai perancangan jaringan *failover* yang akan diterapkan

di PT. Titipan Kilat Riau. Perancangan topologi fisik jaringan *failover* dengan menggunakan jaringan *wireless point-to-point* sebagai koneksi utama dan jaringan internet VPN sebagai koneksi *backup* untuk menghubungkan jaringan kantor cabang dengan jaringan kantor pusat secara lokal (Purnomo, 2013). Pada penerapan *failover*, diimplementasikan menggunakan *static routing* untuk menentukan jalur koneksi yang dikontrol melalui *router* mikrotik. Mekanisme *routing* merupakan penjaluran sebuah data dalam suatu jaringan yang terdiri dari 2 (dua) jenis, yaitu: *static routing* dan *dynamic routing* yang memiliki beberapa tipe *routing protocol* (Joestin, 2015).

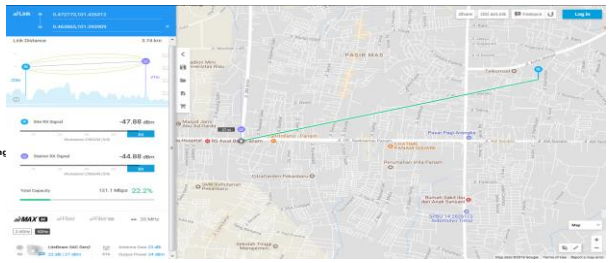


Gambar 5. Desain Topologi Logis Jaringan *Failover*

Perancangan jaringan secara fisik yang terdiri dari perangkat-perangkat jaringan komputer yang saling terhubung satu sama lain, pada masing-masing kantor memiliki jaringan LAN yang terhubung dan dikelola oleh administrator menggunakan router mikrotik. Penggunaan mikrotik memiliki keunggulan diantaranya router jaringan, firewall, VPN server dan client, kualitas pelayanan, pengatur bandwidth dan fungsi-fungsi terkair jaringan komputer (Rachman, 2014; Fitriastuti, 2014). Pada masing-masing router mikrotik terhubung pada sebuah perangkat *wireless* radio pada tower yang terkoneksi secara *wireless point-to-point* dimana perangkat *wireless* radio pada kantor pusat sebagai *access point* (AP) dan *wireless* radio pada kantor cabang sebagai station. Kemudian pada masing-masing *router* mikrotik memiliki koneksi ke jaringan internet dan melalui jaringan *public* internet, router kantor cabang dan router kantor pusat terkoneksi menggunakan jalur *tunnel* VPN dimana pada sisi kantor pusat sebagai VPN *server* dan pada sisi kantor cabang sebagai VPN *client*.

3. Pengembangan (*Development*)

Simulasi *wireless point-to-point* dilakukan menggunakan data yang telah di kumpulkan sebelumnya sebagai parameter dalam simulasi. Media yang digunakan adalah memanfaatkan sistem yang telah di sediakan oleh ubiquiti yang dapat diakses melalui web browser dengan alamat url: *https://link.ubnt.com*. Dalam sistemnya parameter yang harus di tentukan adalah titik koordinat lokasi *Wireless* AP (*Access Point*) yaitu lokasi kantor pusat dan titik koordinat lokasi *Wireless Station* yaitu lokasi kantor cabang kemudian menentukan perangkat *wireless* radio yang digunakan dan ketinggian masing-masing perangkat radio *wireless*.



Gambar 6. Simulasi *Wireless Point-to-Point*

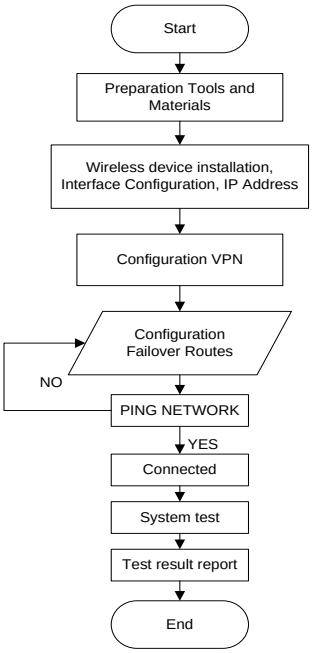
Pada gambaran simulasi diatas hasil yang diperoleh adalah *Link distance* yaitu jarak dari kantor cabang ke kantor pusat adalah 3,74 km, site Rx Signal -47,88 dBm, Station Rx Signal -44,88 dBm dan total capacity 121 Mbps yang dapat melewati jaringan *wireless point-to-point*.

4. Implementasi (*Implementation*)

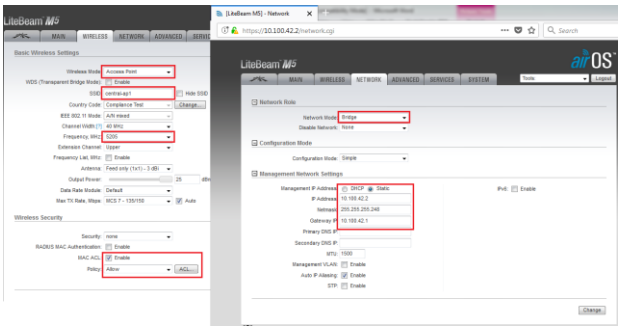
Adapun rencana konsep kerja pada implementasi jaringan *failover* dapat dijabarkan pada *flowchart* yang digambarkan pada Gambar 7.

Konfigurasi Wireless Point-to-Point

Implementasi *wireless point-to-point* ini mencakup tentang instalasi perangkat wireless radio yang dipasang pada masing-masing kantor yang dikoneksikan secara *point-to-point* dimana satu perangkat *wireless* radio sebagai pengirim (*transmitter*) dan satu lagi sebagai penerima (*receiver*). Jaringan *wireless point-to-point* digunakan sebagai jalur utama yang menghubungkan jaringan kantor cabang ke jaringan kantor pusat.



Gambar 7. *Flowchart* Implementasi *Failover*



Gambar 8. Konfigurasi *Wireless* Radio *Ubiquity*

Konfigurasi diatas bertujuan untuk memfungsikan *wireless* radio sebagai *Access Point* dan menetukankan SSID yang berfungsi untuk membedakan satu jaringan WLAN dengan jaringan WLAN lainnya dengan konfigurasi sebagai berikut:

Wireless Mode : Access Point
SSID : central-ap1
Frequency : 5275 MHz
MAC ACL Allow : Enable
Network Mode : Bridge
IP Address : 10.100.42.2
Netmask : 255.255.255.248
Gateway : 10.100.42.1

Selanjutnya pada sisi kantor cabang dilakukan instalasi perangkat *wireless* radio *station* yang merupakan perangkat *wireless* yang bertindak sebagai penerima (*receiver*) dengn konfigurasi sebagai berikut:

Wireless Mode : Station
SSID : central-ap1
Lock to AP : (*MAC Address Wireless AP*)
Frequency : 5275 MHz
Network Mode : Bridge
IP Address : 10.100.42.3
Netmask : 255.255.255.248
Gateway : 10.100.42.4

Kemudian dari masing-masing perangkat *wireless* radio dihubungkan ke *router* mikrotik yang terdapat pada kantor.

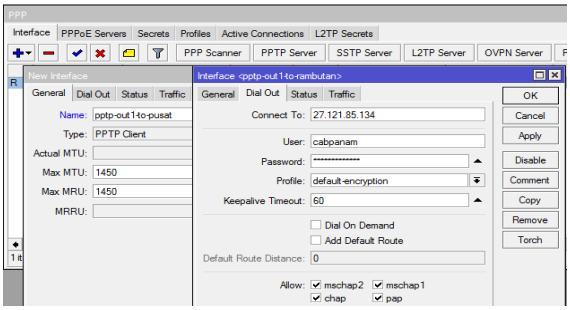
Konfigurasi VPN

Berdasarkan desain jaringan *failover* yang di rancang sebelumnya, koneksi VPN adalah sebagai jalur *backup* untuk menghubungkan jaringan kantor cabang ke kantor pusat. Pada kantor pusat memiliki *bandwidth dedicated* 3 Mbps dan *ip public static* sehingga jalur VPN akan lebih stabil sebagai VPN *Server*. Konfigurasi VPN pada *router* mikrotik kantor pusat dengan mengaktifkan (*enable*) PPTP *Server* dan menambahkan *autentikasi client* PPTP yang akan terkoneksi ke PPTP *server* sebagai berikut:

```
/interface pptp-server server
set enabled=yes
/ppp secret
add          local-address=10.100.41.5
name=cabpanam       password=********
profile=default-encryption    remote-
address=10.100.41.6 service=pptp
```

Selanjutnya konfigurasi VPN *Client* dilakukan pada sisi *router* mikrotik kantor cabang dengan menambahkan *interface* PPTP *Client* untuk membentuk *link virtual* melalui jaringan *public* internet dan *autentikasi* yang terdaftar sebelumnya dengan konfigurasi sebagai berikut.

```
/interface pptp-client
add          connect-to=27.121.85.134
disabled=no   name=pptp-out1-to-pusat
user=cabpanam password=********
```



Gambar 9. Konfigurasi PPTP *Client*

Setelah proses *autentikasi* maka akan terbentuk sebuah *link* PPTP dan pada sisi *client* dan *server* secara otomatis akan diberikan alamat *ip address*.

Konfigurasi *Failover*

Pada tahap konfigurasi jaringan *failover* dilakukan pada *router* mikrotik yang akan menghubungkan antar perangkat jaringan dan mengatur jalur lalu lintas jaringan komputer.

Konfigurasi IP Address

Dengan adanya penambahan koneksi *wireless point-to-point* dilakukan perubahan konfigurasi disisi router mikrotik masing-masing kantor agar perangkat *wireless* AP maupun Station dapat terhubung ke jaringan melalui port *ethernet* pada mikrotik.

Pada router mikrotik kantor pusat penambahan *ip address* sebagai berikut:

```
/ip address
add            address=10.100.42.1/29
interface=ether2-to-panam
network=10.100.42.0
```

Kemudian pada router mikrotik kantor cabang yaitu:

```
/ip address
add            address=10.100.42.4/29
interface=ether2-to-rambutan
network=10.100.42.0
```

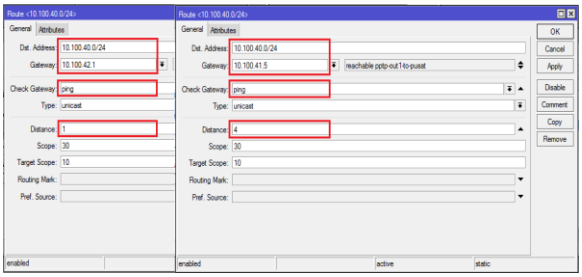
Konfigurasi Routes

Pada konfigurasi *failover* dilakukan *routing* bertujuan untuk menentukan jalur koneksi yang dilalui secara *static*. Pada penelitian ini terdapat dua jalur koneksi yang menghubungkan jaringan kantor pusat dengan jaringan kantor cabang yang dikonfigurasi secara *failover* sehingga apabila *koneksi wireless point-to-point* mengalami masalah atau putus, secara otomatis koneksi akan berpindah ke koneksi VPN, dan apabila koneksi utama sudah pulih seperti sedia kala, maka koneksi akan berpindah secara otomatis ke koneksi utama.

Konfigurasi pada sisi router mikrotik kantor pusat dengan tujuan kantor cabang adalah sebagai berkut:

```
/ip route
add  check-gateway=ping  comment=VPN-
Route          distance=4          dst-
address=10.100.50.0/24
gateway=10.100.41.6
```

```
add  check-gateway=ping  comment=WPTP-
Route          distance=1          dst-
address=10.100.50.0/24 gateway=10.100.42.4
```



Gambar 10. Konfigurasi Routes

Pada *routing* dari kantor cabang ke kantor pusat melakukan konfigurasi sebagai berikut:

```
/ip route
add distance=1 gateway=192.168.1.254
add  check-gateway=ping  comment=VPN-
Route          distance=4          dst-
address=10.100.40.0/24
gateway=10.100.41.5
add check-gateway=ping comment=WPTP-
Route          distance=1          dst-
address=10.100.40.0/24
gateway=10.100.42.1
```

Bila konfigurasi menggunakan tools winbox, yaitu tools yang disediakan oleh mikrotik untuk melakukan remote terhadap router tersebut dapat dilihat pada gambar 11.

Konfigurasi Netwatch

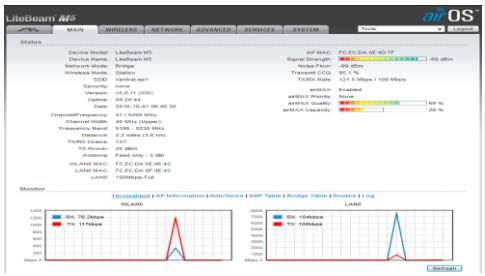
Pada penelitian ini konsep kerja netwatch adalah melakukan *monitoring* terhadap *link* utama *wireless point-to-point* dengan mengirim *ping*. Pada kondisi *host* mengalami *down* maka *netwatch* secara otomatis menjalankan *script* yang berfungsi untuk menonaktifkan (*disable*) *routing* jalur utama sehingga dengan cepat koneksi akan beralih ke jalur *backup* VPN kemudian pada kondisi *host* kembali *up* maka *netwatch* akan menjalankan *script* untuk kembali mengaktifkan (*enable*) *routing* jalur utama sehingga koneksi secara otomatis kembali ke jalur utama *wireless point-to-point*. Konfigurasi pada netwatch sebagai berikut:

```
/tool netwatch
add down-script=":if ([/ip route get
[/ip  route  find  comment=\"WPTP-
Route\"] disabled]=no) do={/ip route
disable     [/ip     route     find
comment=\"WPTP-Route\"]}"
host=10.100.42.1 interval=3s
add host=10.100.42.1 interval=3s up-
script=":if  ([/ip  route  get  [/ip
route  find  comment=\"WPTP-Route\"]
```

```
disabled]=yes) do={/ip route enable
[/ip route find comment="WPTP-
Route\"]}"
```

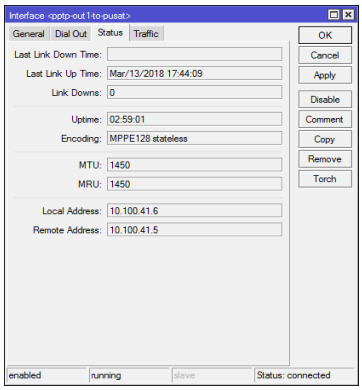
5. Evaluasi (*Evaluation*)

Pada tahapan evaluasi dilakukan *monitoring* terhadap implementasi yang telah dilakukan dan memastikan telah sesuai dengan desain yang telah dirancang sebelumnya. *Monitoring* jalur koneksi *wireless point-to-point* oleh administrator jaringan dengan pengecekan *traffic* pada perangkat *wireless* radio.

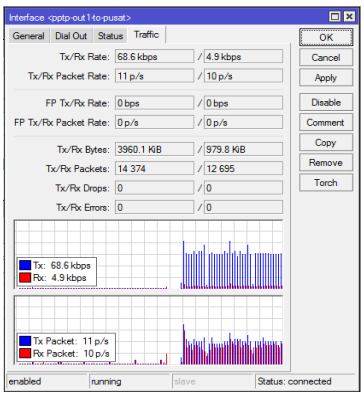


Gambar 11. *Monitoring Main Status Wireless* Radio

Monitoring selanjutnya adalah pada VPN *status* koneksi antara *router* kantor cabang dengan *router* kantor pusat yang melalui jaringan internet.



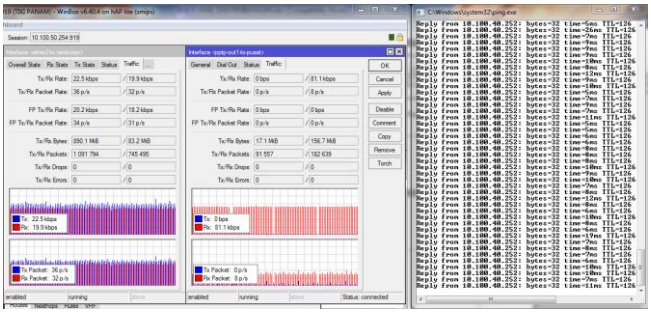
Gambar 12. *Monitoring* VPN *Status*



Gambar 13. *Monitoring* VPN *Traffic*

a. Pengujian dan Hasil

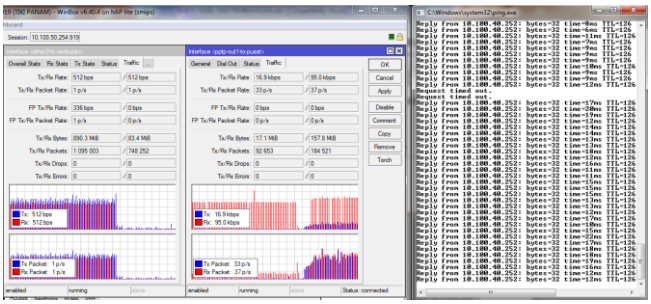
Pada pengujian ini dilakukan untuk melihat kinerja *failover* menggunakan dua jalur koneksi jaringan dalam menjaga interkoneksi jaringan kantor cabang dan kantor pusat tetap terhubung. Pada implementasinya jaringan *wireless point-to-point* adalah sebagai jalur koneksi utama dan jaringan VPN digunakan sebagai jalur koneksi *backup*.



Gambar 14. *Traffic* pada Jalur Koneksi Utama

Pada gambar 14 merupakan traffic data pada kondisi jalur utama dalam keadaan normal terlihat seluruh koneksi melalui *interface* ether2 yang merupakan jaringan *wireless point-to-point*, dan *ping* dengan destination *ip address* dari server yang berada pada jaringan kantor pusat terkoneksi dengan baik.

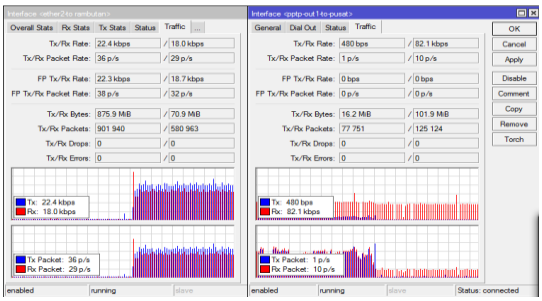
Selanjutnya dalam melakukan pengujian *failover* dilakukan dengan simulasi putusnya koneksi jalur utama sehingga dapat dilihat bagaimana kinerja jaringan *failover* dalam melakukan perpindahan koneksi dari jalur utama ke koneksi jalur *backup*.



Gambar 15. *Traffic* pada Jalur Koneksi *Backup*

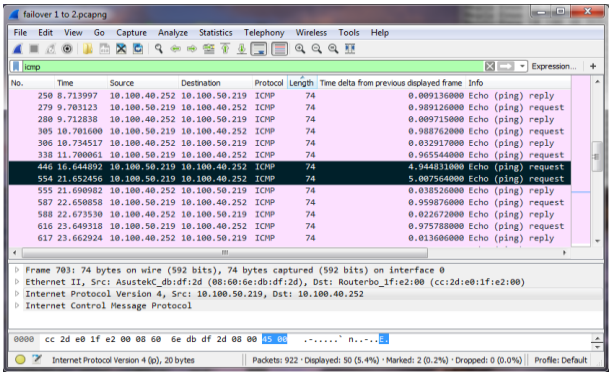
Gambar 15 menunjukkan hasil pengujian saat kondisi jalur utama mengalami putus, maka secara otomatis koneksi akan beralih ke jalur *backup*. Dari hasil pengujian terlihat *traffic* lalu lintas data dari jalur utama berpindah ke jalur *backup* yaitu jaringan VPN seperti pada gambar diatas. Kemudian pada ping terlihat adanya beberapa *time out* dikarenakan

adanya jeda waktu saat perpindahan dari koneksi jalur utama ke jalur koneksi *backup*. Kemudian *delay time* yang menggunakan jaringan *wireless point-to-point* berkisar 1digit sedangkan yang menggunakan VPN berkisar 2 digit.



Gambar 16. *Traffic* Kembali pada Jalur Koneksi Utama

Kemudian apabila jalur utama kembali normal maka secara otomatis koneksi akan berpindah kembali melalui jalur utama jaringan *wireless point-to-point* dan waktu yang dibutuhkan untuk dilakukannya *failover* tidak membutuhkan waktu yang lama.



Gambar 17. Hasil Pengujian *Delay Failover*

Pada pengujian *delay* dilakukan pada saat pengujian *failover* berlangsung dengan melakukan *capture packet* menggunakan *software* wireshark untuk dapat melihat *delay* pada jeda waktu perpindahan dari koneksi jalur utama ke koneksi jalur *backup*. Pada gambar diatas terlihat adanya beberapa time out yang terjadi dengan hasil *delay* yang dapat dilihat pada kolom *time delta from previous displayed frame* dan rata-rata delay sebagai berikut :

$$Delay = \frac{Total\ Delay}{Jumlah\ Total\ Packet}$$

$$Delay = \frac{4.944831 + 5.007564}{2}$$

$$Delay = 4.976197 \text{ s}$$

$$Delay = 4976.197 \text{ ms}$$

IV. PENUTUP

Kesimpulan

Mekanisme koneksi alternatif yang dibangun melalui jaringan *wireless point-to-point* dan jaringan VPN (*Virtual Private Network*) sangat membantu dalam menjaga koneksi dari kantor cabang ke kantor pusat tetap terhubung dikarenakan adanya jalur *backup* apabila koneksi utama mengalami gangguan atau putus. Selain itu, *failover* yang dapat di-*control* melalui mikrotik sangat membantu dalam meningkatkan kinerja perusahaan dan dari sisi perpindahan koneksi dari koneksi utama ke koneksi *backup* tidak memerlukan campur tangan manusia, semua dikerjaan oleh mesin.

Pada simulasi *failover network* ini menunjukkan hasil yang cukup memuaskan terlihat dari kinerja perpindahan jaringan komunikasi dengan tidak membebani *traffic*. Penerapan metode ini juga dapat beroperasi tanpa melibatkan manusia. Pengukuran jeda waktu yang dibutuhkan pada perpindahan jalur koneksi memiliki nilai rata-rata delay tidak lebih dari 4.97 detik.

Saran

Setelah melakukan perancangan, pembangunan dan pengujian maka saran-saran yang mungkin bermanfaat dalam pengembangan selanjutnya antara lain:

1. Untuk meningkatkan kualitas jaringan *wireless point-to-point*, *wireless* radio dapat menggunakan spesifikasi yang lebih tinggi dan memaksimalkan *pointing* antara perangkat *wireless*.
2. Untuk meningkatkan kualitas jaringan VPN membutuhkan *bandwidth* yang cukup besar.

Pengembangan lainnya dalam menurunkan *delay* dapat diterapkan metode *load balancing* pada penelitian selanjutnya dan meningkatkan kualitas jaringan komputer.

V. DAFTAR PUSTAKA

Allen A. Jostein, Meicsy E.I. Najoan, Pinrolinvic D.K. Manembu. (2016). Perancangan Routing Protocol di Jaringan PT. Kawanua Internetindo. *Jurnal Teknik Elektro dan Komputer*, 04(04). ISSN 2301-8402.

Fitriastuti, F., & Utomo, D.P. (2014). Implementasi Bandwidth Management dan Firewall System

Menggunakan Mikrotik OS 2.9.27. *Jurnal Teknik Informatika*, 04(01). ISSN: 2088-3676.

Harsapranata, A.I. (2014). Implementasi Failover Menggunakan Jaringan VPN dan Metronet pada Astridogroup Indonesia, *Jurnal Teknik dan Ilmu Komputer*, 08(02). ISSN: 1978-8282.

Iskandar, I., & Hidayat, A. (2015). Analisa Quality of Service (QoS) Jaringan Internet Kampus (Studi Kasus: UIN Suska Riau). *Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, 01(02). ISSN: 2460-738X.

Kadir, A., & Tone, K. (2015). Analisa Kerja Access Point Jaringan Wireles pada Universitas Al Asyariah Mandar. *Jurnal Ilmu Komputer*, 01(01). ISSN: 2442-4512.

Mukhtar, H., Hafid, A., & Wenando, F.A. (2017). Local Network Communication Based on Virtual Private Network (VPN) at Universitas Muhammadiyah Riau. Paper presented at *the International Conference of Applied Science on Engineering, Business, Linguistics and Information Technology (ICo-ASCNITech)*, Padang, 13-15 Oktober 2017. ISSN 2598-2532.

Mrs. Swapna, G., Sri Naga Sri, G., Nikila Santha Kumari, N., & Sravani Devi, N. (2017). Secure Connection in VPN using AES. *International Research Journal of Engineering and Technology (IRJET)*, 04(04). ISSN 2395-0056.

M.Z. Oba, A.A. Ayeni. (2016). Data Rates Performance Analysis of Point to Multi-Point Wireless Link in University of Ilorin Campus. *International Research Journal of Engineering and Technology (IRJET)*, 03(01). ISSN: 2395-0056.

Palaha, F., & Zaini. (2014). Propagasi Indoor Gelombang Radio Perangkat Xbee di Rumah Sakit Ibu dan Anak Budhi Mulia Pekanbaru. Jurnal Nasional Teknik Elektro, 03(02). ISSN: 2302-2949.

Pribadi, P.T. (2013). Implementasi High-Availability VPN client pada jaringan komputer Fakultas Hukum Universitas Udayana, Jurnal Ilmu Komputer – Vol. 6 No. 1, Universitas Udayana.

Purnomo, N., Syafrizal, M. (2013). Failover Cluster Server dan Tunneling EoIP untuk Sistem Disaster Recovery. Paper presented *at Seminar Nasional Teknologi Informasi dan Multimedia 2013*, Yogyakarta, 19 Januari 2013. ISSN: 2302-3805.

Rachman, A., Mukminin, M., Huda, M., Safynatun, N., Cendra, F.S. (2014). Integrasi Mikrotik dan Wireless Radio Sebagai Media Efisiensi Internet di Perusahaan. *Jurnal Lontar Komputer*, 05(01). ISSN: 2088-1541.

Sopandi, D. (2008). *Instalasi dan Konfigurasi Jaringan Komputer*. Bandung: Informatika.

Sukmaaji, A., & Rianto. 2008. *Jaringan komputer*. Yogyakarta: Andi Offset

Triyono, J., Rachmawati K., R. Y., & Irnawan, F. D. (2014). Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data. *Jurnal Jarkom*, 01(02). ISSN: 2338-6312.

Varianto, E., & Badrul. M. (2015). Implementasi Virtual Private Network dan Proxy Server menggunakan Clear OS pada PT. Valdo International. *Jurnal Sistem Informasi*, 01(01). ISSN: 2442-2436.

Zamzami, N. F. (2013). Implementasi Load Balancing dan Failover menggunakan Mikrotik RouterOS berdasarkan multihomed gateway pada warung internet "DIGA". Skripsi, Universitas Dian Nuswantoro, Semarang, Indonesia.