Jurnal Teknik Komputer AMIK BSI
Volume 7, No.2, Juli 2021
P-ISSN 2442-2436, E-ISSN: 2550-0120
Akreditasi Ristekdikti, No: 36/E/KPT/2019 (Sinta 4)
DOI: 10.31294/jtk.v4i2

Implementasi *Virtual Private Network Failover* Menggunakan Mikrotik Pada Jaringan Lokal Politeknik Negeri Sriwijaya

Muhammad Munaza Fathsyah[1], Irawan Hadi[2], Irma Salamah[3]

[1,2,3]Teknik Elektro, Teknik Telekomunikasi, Politeknik Negeri Sriwijaya, Kota Palembang, Indonesia
[1]e-mail: nazadewa39@gmail.com
[2]e-mail: irawanhadi657@yahoo.com
[2]e-mail: irma.salamah@yahoo.com

Diterima	Direvisi	Disetujui
27-07-2021	28-07-2021	30-07-2021

Abstrak - Pertumbuhan, perkembangan, dan kebutuhan akan informasi terus-menerus menjadi sebuah kebutuhan primer bagi setiap masyarakat umum, organisasi, perusahaan, dan lembaga pendidikan. Salah satu contoh lembaga pendidikan yang memiliki kebutuhan akan informasi yaitu Politeknik Negeri Sriwijaya (Polsri), dimana dosen dan mahasiswa memerlukan koneksi melalui sebuah media kabel ataupun nirkabel untuk terhubung ke jaringan internet (global) maupun jaringan intranet (lokal). Sistem Akademik dan *Learning Management System* (LMS) adalah salah satu jaringan lokal Polsri yang paling sering diakses untuk memenuhi kegiatan akademik. Dosen ataupun mahasiswa sebagai *client* akan terus dapat mengakses jaringan lokal tersebut selama jalur komunikasi atau media transmisi antar *router client* dan *router server* tetap terhubung. Apabila jalur komunikasi utama antar *router client* dan *router server* terputus oleh faktor tertentu, maka *client* tidak dapat mengakses jaringan lokal sehingga proses kegiatan akademik menjadi terhambat. Untuk menghindari kejadian tersebut, maka diperlukan sebuah jalur komunikasi cadangan (*backup link*) dan suatu penerapan teknik *failover* pada sisi *router client*. Teknik *failover* adalah teknik yang memiliki kemampuan untuk mengalihkan jalur komunikasi utama ke jalur komunikasi cadangan sehingga komunikasi dapat terus berjalan meskipun jalur komunikasi utama terputus. Jalur komunikasi cadangan pada implementasi ini didukung oleh teknologi telepon seluler generasi keempat atau teknologi yang lebih dikenal dengan istilah 4G LTE (*Fourth Generation Long Term Evolution*). Selain itu, terdapat penerapan *Virtual Private Network* (VPN) tipe *Layer Two Tunneling Protocol* (L2TP) pada jalur komunikasi cadangan untuk menjaga keamanan komunikasi. Protokol *routing* yang akan digunakan untuk melakukan proses pertukaran informasi *routing* pada implementasi ini adalah *Border Gateway Protocol* (BGP).

Kata Kunci: *Failover*, Mikrotik, *Virtual Private Network*

Abstract *- The growth, development, and need for information continues to be a primary need for every general public, organization, company, and educational institution. One example of an educational institution that has a need for information is the Sriwijaya State Polytechnic (Polsri), where lecturers and students need a connection to connect to the internet network or local network. The Academic System and Learning Management System (LMS) is one of the most frequently accessed local Polsri networks to fulfill academic activities. Lecturers or students as clients will continue to be able to access the local network as long as the communication line or transmission medium between the client router and server router remains connected. If the main communication line between the client router and server router is interrupted by certain factors, the client cannot access the local network. To avoid this incident, we need a backup communication line and an application of failover techniques on the client router side. The failover technique is a technique that has the ability to switch the main communication line to a backup communication line so that communication can continue even though the main communication line is disconnected. The backup communication line supported by 4G LTE (Fourth Generation Long Term Evolution). In addition, there is the application of a Layer Two Tunneling Protocol (L2TP) Virtual Private Network (VPN) on the backup communication line to maintain communication security. The routing protocol that will be used to exchange routing information in this implementation is the Border Gateway Protocol (BGP).*

Keywords: Failover, Mikrotik, Virtual Private Network

PENDAHULUAN

Saat ini teknologi telekomunikasi mengalami perkembangan yang sangat pesat. Teknologi telekomunikasi sudah menjadi kebutuhan primer yang dapat mendukung berbagai kegiatan manusia sehingga dapat berjalan dengan cepat. Teknologi telekomunikasi saat ini sangat didukung oleh media transmisi serat optik (*fiber optic*) yang dapat menyalurkan informasi dengan kapasitas besar dan keandalan tinggi dalam waktu yang sangat singkat. Serat optik menjadi media transmisi bawah laut yang menghubungkan telekomunikasi antar negara-negara sehingga membentuk jaringan komunikasi secara global dan terbuka atau yang lebih dikenal dengan jaringan internet.

Lembaga pendidikan Politeknik Negeri Sriwijaya (Polsri) adalah salah satu contoh lembaga pendidikan dimana dosen dan mahasiswa membutuhkan koneksi untuk terhubung ke jaringan internet (global) ataupun intranet (lokal). Kebutuhan akan koneksi ke jaringan global ataupun lokal ini diperuntukkan untuk menunjang kegiatan akademik seperti pembelajaran selama proses perkuliahan berlangsung. Jaringan lokal yang diakses oleh dosen ataupun mahasiswa Polsri tersebut meliputi Sistem Akademik dan *Learing Management System* (LMS) yang digunakan untuk menunjang kegiatan akademik seperti absensi dosen dan mahasiswa, pengumpulan tugas, dan mengunduh materi pembelajaran.

Polsri sendiri menggunakan jalur komunikasi atau media transmisi serat optik antar *router client* dan *router server* sehingga dapat melakukan komunikasi yang cepat dengan kapasitas yang besar. Akses jaringan lokal yang dilakukan oleh dosen ataupun mahasiswa akan terus berjalan selama koneksi jalur komunikasi utama antar *router client* dan *router server* tetap terhubung. Apabila jalur komunikasi utama (*main link*) antar *router client* dan *router server* terputus oleh faktor tertentu, maka dosen dan mahasiswa yang terhubung pada *router client* melalui media kabel ataupun nirkabel tidak dapat mengakses jaringan lokal sehingga beberapa bentuk kegiatan akademik tidak dapat terpenuhi. Untuk mengantisipasi hal tersebut, maka dibutuhkan sebuah jalur komunikasi cadangan (*backup link*) dan penerapan teknik *failover* pada sisi *router client*.

Teknik *failover* adalah teknik yang mampu untuk mengalihkan jalur komunikasi utama ke jalur komunikasi cadangan (alternatif) sehingga komunikasi dapat terus berjalan meskipun jalur komunikasi utama antar *router client* dan *router server* terputus (Harsapranata, 2015). Teknik *failover* biasanya digunakan pada cabang kantor sebuah perusahaan yang membutuhkan koneksi terhadap kantor pusatnya. Apabila jalur komunikasi utama suatu cabang kantor perusahaan terputus terhadap kantor pusatnya, maka semua aplikasi yang harus dikerjakan oleh tenaga kerja di kantor cabang tersebut akan berhenti. Teknik *failover* juga sangat baik digunakan pada mesin ATM (*Automated Teller Machine*) sehingga dapat terus berinteraksi dengan pengguna meskipun jalur komunikasi utama mesin ATM terhadap lembaga keuangan pusatnya telah terputus. Pada dasarnya, teknik *failover* diimplementasikan pada suatu jaringan yang tidak ingin mengalami *downtime*.

Pada penelitian kali ini, implementasi *failover* akan diterapkan pada jaringan lokal Polsri dimana *router client* dapat mengalihkan jalur komunikasi utama (*fiber optic*) menjadi jalur komunikasi cadangan apabila komunikasi terhadap *router server* terputus. Jalur komunikasi cadangan pada implementasi ini didukung oleh teknologi telepon seluler 4G LTE (*Fourth Generation Long Term Evolution*) dengan menggunakan Modem (Modulator Demodulator). Selain itu, pada implementasi kali ini terdapat penerapan *Virtual Private Network* (VPN) tipe *Layer Two Tunneling Protocol* (L2TP) pada jalur komunikasi cadangan untuk komunikasi yang lebih aman. Protokol *routing* yang akan digunakan untuk melakukan proses pertukaran informasi *routing* antar *router client* dan *router server* pada implementasi kali ini adalah *Border Gateway Protocol* (BGP).

Cara kerja implementasi ini yaitu apabila komunikasi antar *router client* dan *router server* terputus, maka *router client* akan mengalihkan jalur komunikasi utama ke jalur komunikasi cadangan (4G LTE) sehingga *router client* tetap dapat mengakses jaringan internet. Melalui jaringan internet inilah *router client* akan terhubung pada VPN *Concentrator* yang dimiliki oleh *router server* sehingga membentuk suatu jalur komunikasi virtual baru. Kemudian proses pertukaran informasi *routing* antar *router client* dan *router server* dilakukan melalui jalur komunikasi virtual baru tersebut menggunakan BGP.

METODOLOGI PENELITIAN

Metode penelitian yang digunakan kali ini yaitu *Research and Development* (R&D) dimana terdapat banyak penelitian sebelumnya yang berhubungan dengan penelitian yang akan dibahas. Penelitian-penelitian sebelumnya banyak menggunakan media transmisi serat optik (fiber optic) sebagai jalur komunikasi utama maupun jalur komunikasi cadangan. Jalur komunikasi cadangan pada penelitian ini menggunakan teknologi telepon seluler 4G LTE dan penerapan VPN tipe L2TP sehingga proses pertukaran data tetap aman dan tidak diketahui oleh pihak ketiga yang tidak memiliki wewenang.

Gambar 1. Metodologi Penelitian
Sumber: (Fathsyah, 2021)

1. Studi Pustaka
Merupakan pengumpulan data dengan cara membaca referensi dari jurnal, buku, dan berbagai laporan yang berkaitan dengan penelitian yang akan dibahas oleh penulis.

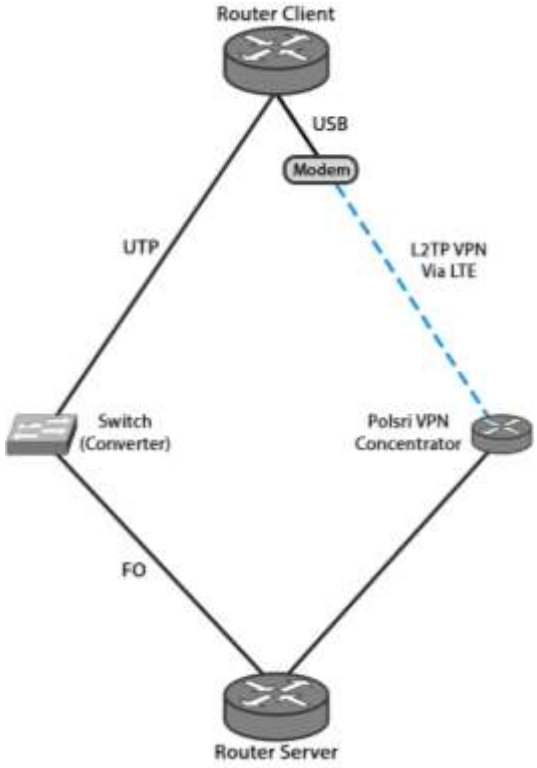
2. Perancangan Topologi dan Instalasi Perangkat
Merupakan proses merancang suatu susunan jaringan yang akan dibangun dan selanjutnya akan diimplementasikan pada keadaan yang sebenarnya.

3. Konfigurasi Perangkat
Merupakan proses pembuatan suatu pengaturan pada perangkat (*router*) seperti alokasi alamat IP, *Network Address Translation* (NAT), *routing*, *peering*, dan konfigurasi lainnya yang berhubungan dengan penelitian yang akan dibahas.

4. Analisa Sistem
Merupakan penguraian tentang hasil penelitian dengan mengetahui bagaimana komponen jaringan tersebut bekerja dengan satu sama lain untuk mencapai hasil yang diharapkan.

HASIL DAN PEMBAHASAN

1. Perancangan Topologi
Topologi jaringan merupakan suatu sistem yang dibuat untuk menghubungkan suatu jaringan dengan menggunakan unsur-unsur seperti *router, link, switch, hub*, dan komputer. Topologi jaringan memudahkan teknisi untuk melihat bagaimana gambaran untuk membangun jaringan yang diinginkan. Berikut adalah topologi jaringan *failover* yang akan diimplementasikan pada jaringan lokal Polsri.



Gambar 2. Topologi *Failover* Jaringan Lokal Polsri
Sumber: (Fathsyah, 2021)

2. Instalasi Perangkat
Untuk mengantisipasi jaringan agar tidak mengalami kendala atau kesalahan sebelum penerapan pada *router client* yang sebenarnya, maka penelitian ini akan membuat sebuah jaringan uji coba menggunakan salah satu jalur (*core*) yang tidak digunakan pada salah satu gedung kuliah Polsri (*client*) sebagai *dummy network*. Pada penelitian kali ini, *router* yang digunakan pada sisi *client* adalah Routerboard RB951Ui-2nD dengan lima *port* ethernet serta tidak memiliki *port* SFP (*Small Form-Factor Pluggable*). Oleh karena itu, diperlukan sebuah *converter* atau *switch* (*ethernet to fiber optic*) sehingga Routerboard *client* ini dapat melakukan komunikasi terhadap *router client*. *Converter* ataupun *switch* tidak diperlukan apabila Routerboard yang digunakan telah memiliki *port* SFP. Selain itu,

perangkat SFP juga diperlukan sebagai *transceiver* menggunakan media serat optik.
Dapat dilihat pada topologi jaringan diatas dimana Routerboard terhubung ke *switch* melalui media kabel UTP (*Twisted Pair*) terlebih dahulu sebelum terhubung ke *router server* melalui media serat optik. Jalur komunikasi cadangan menggunakan Modem yang sudah ada kartu SIM (*Subscriber Identity Module*) didalamnya akan dihubungkan pada *router client*. Apabila Routerboard terhubung pada suatu Modem maka *Internet Service Provider* (ISP) yang bersangkutan akan memberikan alamat IP pada *interface* lte1 yang terdapat pada Routerboard secara dinamis.

Gambar 3. Tampak Perangkat Penelitian
Sumber :(Fathsyah, 2021)

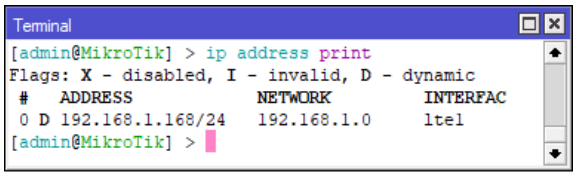
3. Konfigurasi Perangkat

Pada bagian ini, terdapat tahap-tahap konfigurasi pada sisi *router client* dan *router server* dan sedikit penjelasan tentang konfigurasi apa yang telah dibuat. Hal pertama yang harus dilakukan adalah membuat suatu *interface bridge* pada kedua sisi *router* yang nantinya akan digunakan sebagai *backup link*.

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

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

Selanjutnya mengalokasikan alamat IP pada seluruh *interface* yang akan digunakan seperti ether1 (*main link*), bridge1 (*backup link*), dan wlan1 (*accsess point*) pada sisi *router client*. I*nterface* lte1 (LTE/internet) otomatis akan masuk pada *interface list* apabila *router client* sudah terhubung dengan Modem sehingga tidak perlu mengalokasikan alamat IP lagi.



Gambar 4. *Interface* LTE Pada *Router Client*
Sumber: (Fathsyah, 2021)

Untuk memahami bagaimana sistem *failover* yang terjadi pada *router client*, maka ada baiknya kita menghapus *interface* lte1 (*dynamic*) dan membuat kembali alamat IP untuk *interface* lte1 (*static*).

```
[admin@client] > /ip address remove number=0
[admin@client] > /ip address add address=192.168.1.168/24 interface=lte1 network=192.168.1.0
[admin@client] > /ip address add address=10.1.1.71/25 interface=ether1 network=10.1.1.0
[admin@client] > /ip address add address=10.255.0.2/30 interface=bridge1 network=10.255.0.0
```

```
[admin@server] > /ip address add address=10.255.0.1/30 interface=bridge1 network=10.255.0.0
```

Setelah semua *interface* sudah dialokasikan alamat IP, maka hal yang dilakukan selanjutnya adalah membuat dua buah *default static routing* dengan nilai *distance* yang berbeda. *Default static routing* yang pertama menggunakan *gateway* jalur komunikasi utama dengan nilai *distance* "1" dan *default static routing* yang kedia menggunakan *gateway* jalur komunikasi cadangan (lte1) dengan nilai *distance* "2". Hal lain yang perlu dilakukan yaitu penambahan DNS (*Domain Name System*).

```
[admin@client] > /ip route add gateway=10.1.1.1 distance=1
[admin@client] > /ip route add gateway=192.168.1.1 distance=2
[admin@client] > /ip dns set servers=10.10.1.1,10.10.1.10
```

Perbedaan nilai *distance* pada perintah diatas menunjukan *default gateway* yang mana yang harus didahului oleh *router client*. Semakin kecil nilai *distance* maka *default gateway* tersebut akan diutamakan. Ketika *default gateway* dengan nilai distance "1" terputus (*main link*), maka *router client* akan secara otomatis mengalihkan *default gateway* ke *gateway* dengan nilai *distance* lebih dari "1" (*backup link*). Selanjutnya melakukan pertukaran informasi *routing* antar *router client* dan *router server* menggunakan BGP melalui jalur komunikasi utama. Hal yang perlu dilakukan selanjutnya adalah mengatur ASN (*Autonomous System Number*) pada *router client*.

```
[admin@client] > /routing bgp instance edit number=0 value-name=as
```

Gambar 5. Pengubahan ASN
Sumber: (Fathsyah, 2021)

[admin@client] > /routing bgp peer add comment=FO keepalive-time=10s name="Peer link FO" remote-address=10.1.1.2 remote-as=46047

[admin@server] > /routing bgp peer add keepalive-time=10s name="Peer link FO" remote-address=10.1.1.71 remote-as=64516

Kemudian untuk membuktikan apakah proses pertukaran informasi *routing* menggunakan BGP berhasil, maka perlu dilakukan proses ping (*packet internet gropher*).

Gambar 6. Ping *Server Via Main Link*
Sumber: (Fathsyah, 2021)

Gambar diatas menunjukan bahwa alamat IP yang dituju memberikan respon sehingga *router client* dapat melakukan akses ke jaringan lokal Polsri. Selanjutnya hal yang perlu dilakukan adalah menghubungkan *router client* ke *router server* melalui jalur komunikasi cadangan menggunakan L2TP. Apabila *router server* belum memiliki *server* L2TP, L2TP *secret*, dan L2TP *profile*, maka dapat membuat dengan menggunakan perintah berikut.

[admin@servertest1] > /interface l2tp-server server set enabled=yes
[admin@servertest1] > /ip pool add name=pool1 ranges=192.168.1.2-192.168.1.254
[admin@servertest1] > /ppp profile add name=profile1 local-address=192.168.1.1 remote-address=pool1
[admin@servertest1] > /ppp secret add name=test1 password=test1 service=l2tp profile=profile1

Perintah diatas meliputi perintah untuk mengaktifkan server L2TP, membuat *ranges* alamat IP, *profile* L2TP, *username* dan *password* yang akan digunakan oleh *client*. Pada implementasi kali ini *router server* sudah memiliki *server* L2TP sehingga hanya memerlukan sedikit penambahan konfigurasi pada *router server*, yaitu sebagai berikut.

[admin@server] > /ppp profile set profile1 bridge=bridge1

[admin@client] > /ppp profile set default-encryption bridge=bridge1
[admin@client] > /interface l2tp-client add comment=L2TP connect-to=202.9.69.240 dial-on-demand=yes disabled=no name=l2tp-out1 password=******** user=******** profile=default-encryption use-ipsec=no

Dapat dilihat pada perintah diatas bahwa kedua sisi menambahkan *interface bridge1* pada *profile* di menu PPP (*Point to Point Protocol*). Artinya kedua sisi ini akan membuat segmen baru menggunakan *interface bridge1* pada jalur L2TP. Hal ini dilakukan agar alamat IP pada *tunnel* L2TP bersifat statis sehingga dapat melakukan BGP pada segmen ini. Apabila *router client* terhubung pada *server* L2TP menggunakan alamat IP dinamis yang diberikan oleh *server* tersebut, maka proses *peering* BGP akan terganggu karena memungkinkan alamat IP *router client* akan berubah sewaktu-waktu. *Router client* terhubung pada *server* L2TP Polsri menggunakan *profile* dan *username* serta *password* yang telah ada sehingga beberapa perintah diatas penulis menyamarkannya untuk menjaga rahasia lembaga.

Setelah terbentuk suatu segmen baru menggunakan L2TP, maka perintah terakhir yang dilakukan adalah pertukaran informasi *routing* antar *router client* dan *router server* menggunakan BGP melalui jalur komunikasi cadangan dengan perintah berikut.

[admin@client] > /routing bgp peer add comment=LTE keepalive-time=10s name="Peer link LTE" remote-address=10.255.0.1 remote-as=46047

[admin@server] > /routing bgp peer add keepalive-time=10s name="Peer link LTE" remote-address=10.255.0.2 remote-as=64516

[admin@client] > /routing bgp peer print

Gambar 7. *Peer List* Pada *Router Client*
Sumber: (Fathsyah, 2021)

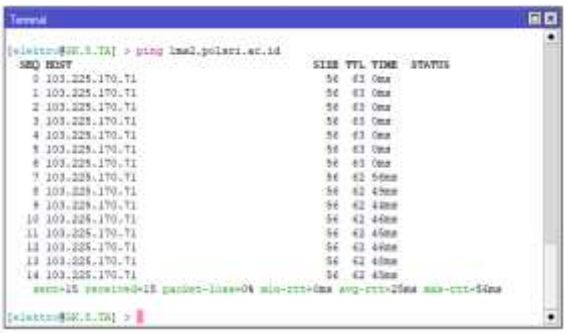
Dapat dilihat pada gambar diatas bahwa terdapat *flags* "E" (*Established*) pada daftar *peer* di sisi *router client* setelah melakukan pertukaran informasi *routing* menggunakan BGP. *Flag* tersebut menunjukan bahwa kedua jalur komunikasi baik jalur komunikasi utama maupun jalur komunikasi cadangan telah saling bertukar informasi *routing*. Adapun perintah tambahan untuk membuat *access point* pada *router client* sehingga client dapat

mengakses jaringan lokal polsri melalui *router client* yang baru saja di konfigurasi.

```
[admin@client] > /ip address add address=10.71.4.254/24 interface=wlan1 network=10.71.4.0
[admin@client] > /ip pool add name=dhcp_pool1 ranges=10.71.4.1-10.71.4.253[admin@client] > /ip dhcp-server add address-pool=dhcp_pool1 disabled=no interface=wlan1 lease-time=1d name=dhcp1
[admin@client] > /interface wireless security-profiles add name=profile1 mode=dynamic-keys authentication-types=wpa-psk,wpa2-psk wpa-pre-shared-key=routerclient wpa2-pre-shared-key=routerclient
[admin@client] > /interface wireless set [find default-name=wlan1] band=2ghz-b/g/n disabled=no frequency=2417 mode=ap-bridge security-profile=profile1 ssid=routerclient wps-mode=disabled
[admin@client] > /ip firewall nat add action=masquerade chain=srcnat out-interface=wlan1
```

4. *Test and Commisioning*

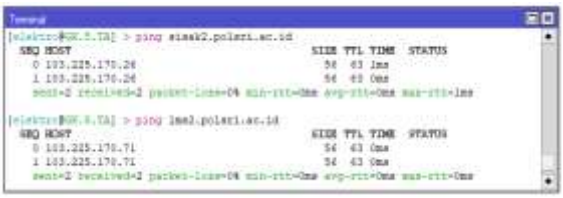
Test and commissioning merupakan tahapan pengujian secara keseluruhan untuk membuktikan apakah implementasi sudah berjalan sesuai dengan apa yang diinginkan atau belum. Pengujian ini meliputi respon *router client* ketika jalur komunikasi utama diputuskan dan respon *router client* saat jalur komunikasi utama dihubungkan kembali. Selain itu, terdapat pengujian dengan cara mengecek respon *server* dengan melakukan ping terhadap salah satu jaringan Polsri melalui jalur komunikasi utama maupun jalur komunikasi cadangan. Pengujian terakhir yaitu melakukan *route tracing* untuk melihat apakah *gateway* jalur komunikasi utama maupun jalur komunikasi cadangan sudah benar berjalan dengan baik atau apakah belum memenuhi kebutuhan. Jika pada saat melakukan *test and commissionong* terdapat sebuah kesalahan, maka diperlukan analisa kembali pada bagian konfigurasi.



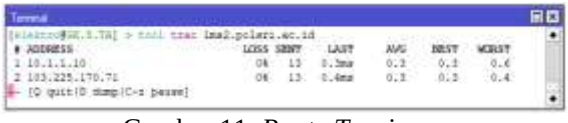
Gambar 8. *Main Link to Backup Link Failover*
Sumber: (Fathsyah, 2021)

Gambar 9. *Backup Link to Main Link Failover*
Sumber: (Fathsyah, 2021)

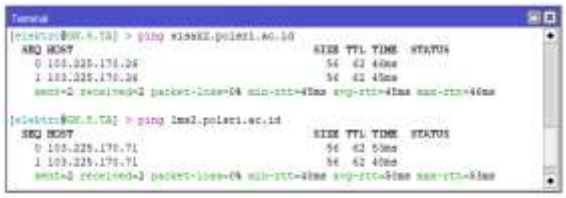
Kedua gambar tersebut menunjukan bahwa pengalihan jalur komunikasi utama ke jalur komunikasi cadangan ataupun sebaliknya sudah sesuai dengan hasil yang diharapkan. Proses pengalihan jalur komunikasi dari kedua gambar diatas dapat diketahui dengan cara melihat perbedaan waktu respon *router server* terhadap *router client*. Waktu respon melalui jalur komunikasi cadangan memiliki selisih waktu sekital 46ms terhadap waktu respon melalui jalur komunikasi utama. Hal ini dikarenakan jalur komunikasi utama menggunakan media serat optik sehingga proses komunikasi menjadi sangat cepat dengan waktu respon kurang dari 1ms, sedangkan jalur komunikasi cadangan menggunakan jaringan telepon seluler dimana proses komunikasi dapat dipengaruhi oleh jarak perangkat atau modem terhadap *Base Transceiver Station* (BTS) yang jauh dan cuaca yang tidak mendukung seperti badai atau hujan. Pengujian terakhir adalah melakukan ping ke jaringan lokal Polsri untuk membuktikan apakah *router client* dapat mengakses jaringan lokal Polsri baik melalui jalur komunikasi utama ataupun jalur komunikasi cadangan. dan melakukan *route tracing* melalui kedua jalur komunikasi antar *router client* dan *router*.



Gambar 10. Ping *Server Local Network Via Main Link*
Sumber: (Fathsyah, 2021)



Gambar 11. *Route Tracing Via Main Link*
(Sumber: (Fathsyah, 2021)



Gambar 12. Ping *Server LocalNetwork Via Backup Link*
Sumber : (Fathsyah, 2021)

Gambar 13. *Route Tracing Via Backup Link*
Sumber : (Fathsyah, 2021)

KESIMPULAN

Failover merupakan teknik yang memiliki kemampuan untuk mengalihkan suatu jalur komunikasi ke jalur cadangan secara otomatis apabila jalur komunikasi utama tersebut terputus. Pada penelitian ini, dapat dilihat bahwa percobaan pengalihan jalur komunikasi utama melalui media serat optik ke jalur komunikasi cadangan melalui jaringan telepon seluler pada *router client* telah berhasil. *Router client* tetap dapat mengakses jaringan lokal polsri seperti mengakses Sistem Akademik dan *Learn Management System* (LMS) meskipun jalur komunikasi utama antar *router client* dan *router server* telah terputus. Selain itu, jalur komunikasi cadangan menggunakan VPN L2TP untuk meningkatkan keamanan komunikasi.

Pada penelitian ini, seluruh aspek seperti pengalihan jalur komunikasi, penerapan VPN L2TP pada jalur komunikasi cadangan, pertukaran informasi *routing* menggunakan BGP pada kedua jalur komunikasi, dan *gateway router client* telah memenuhi hasil yang diharapkan. Kekurangan menggunakan jalur komunikasi cadangan melalui jaringan telepon seluler adalah perbandingan *bandwidth* yang jauh lebih kecil sehingga prosek mengakses jaringan lokal akan melambat apabila diakses oleh *client* secara massal. Adapun saran yang diberikan oleh peneliti kepada pembaca bahwa penerapan *failover* sangat diperlukan untuk mengantisipasi apabila jalur komunikasi utama sebuah jaringan telah terputus dan penerapan ini juga sangat diperlukan untuk suatu organisasi, perusahaan, lembaga pendidikan atau lainnya yang tidak menginginkan jaringannya mengalami *downtime*.

REFERENSI

Adhiwibowo, W., & Irawan, A. R. (2019). Implementasi Redundant Link Untuk Mengatasi Downtime Dengan Metode Failover. *Jurnal Pengembangan Rekayasa Dan Teknologi*, *15*(1), 48. https://doi.org/10.26623/jprt.v15i1.1490

Darojat, A., & Nurhaida, I. (2019). Analisa Qos Administrative Distance. *Jurnal Ilmu Teknik Dan Komputer*, *3*(1), 11–21.

Harsapranata, A. I. (2015). Implementasi Failover Menggunakan Jaringan Vpn Dan Metronet Pada Astridogroup Indonesia. *CCIT Journal*, *8*(2), 66–77. https://doi.org/10.33050/ccit.v8i2.321

Khasanah, S. N., & Utami, L. A. (2018). Implementasi Failover Pada Jaringan WAN Berbasis VPN. *Jurnal Teknik Informatika STMIK Antar Bangsa*, *4*(1), 62–66.

Mohammad Badrul, A. (2019). Implementasi Automatic Failover Menggunakan Router Jaringan Mikrotik Untuk Optimalisasi Jaringan. *Jurnal PROSISKO*, *6*(2), 82–87.

Musril, H. A. (2017). Simulasi Interkoneksi Antara Autonomous System (As) Menggunakan Border Gateway Protocol (Bgp). *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *2*(1), 1–9. https://doi.org/10.30743/infotekjar.v2i1.151

Novianto, D., & Helmud, E. (2019). Implementasi Failover dengan Metode Recursive Gateway Berbasis Router Mikrotik Pada STMIK Atma Luhur Pangkalpinang. *Jurnal Ilmiah Informatika Global*, *10*(1), 26–31. https://doi.org/10.36982/jig.v10i1.732

Ramandito, R., Sumaryono, S., & Kusumawardhani, S. S. (2010). Analisis Performace Jaringan Komputer Dengan Mekanisme Load Balancing-Failover. In *Jurnal Penelitian Teknik Elektro* (Vol. 3, Issue 4, pp. 177–181).

Xie, G. (2006). Naval Postgraduate. *Security*, *December*, 79.

Zamzami, N. F. (2005). Implementasi load balancing dan failover menggunakan mikrotik router os berdasarkan multihomed gateway pada warung internet ”diga”. *Implementasi Load Balancing Dan Failover Menggunakan Mikrotik Router Os Berdasarkan Multihomed Gateway Pada Warung Internet ”diga”*, 12.