IMPLEMENTASI ROUTING OPEN SHORTEST PATH FIRST (OSPF) MELALUI TUNNEL OPEN VPN

Tri Mulyadin[1], Muhammad Sholeh[2], Catur Iswahyudi[3]
[1,2,3,]Teknik Informatika,Institut Sains & Teknologi AKPRIND, Yogyakarta
Email : [1]moeldg@gmail.com, [2]muhash@akprind.ac.id, [3]catur@akprind.ac.id

ABSTRACT

To connect the office with another office in different location, it takes the transmission media for data communication. one of the transmission media that can be used is Open VPN using the internet. OSPF routing required to connect all routers in the network using a VPN.OSPF routing on the Open VPN network, could be a solution for companies who want to build a network to connect multiple offices in different locations with a network.The implementation of OSPF routing in the Open VPN network uses three pieces of routerboard with one public IP. The testing is done by analyzing the process of selection of routing line, analysis of time speed of convergence, analysis of speed is the literature study, simulation to the virtualbox, and implementation to test-bed network.The test results convergence time using the same ISP is55,28 seconds and using a different ISP is 55,seconds. Test results on the routing update process with the same ISP is 7,23 and 9,63 seconds using a different ISP. Overall the OSPF routing on the Open VPN networks able to work well with convergence time and time routing updates fast and up to date

Keywords : *Routing, OSPF, Open VPN*

INTISARI

Untuk menghubungkan kantor dengan kantor lain di lokasi yang berbeda, dibutuhkan media transmisi untuk komunikasi data. Salah satu media transmisi yang dapat digunakan adalah Open VPN menggunakan internet. OSPF routing diperlukan untuk menghubungkan semua router dalam jaringan menggunakan VPN. OSPF routing pada jaringan Open VPN bisa menjadi solusi bagi perusahaan yang ingin membangun jaringan untuk menghubungkan beberapa kantor di lokasi yang berbeda dengan satu jaringan. Implementasi routing OSPF pada jaringan Open VPN menggunkan tiga buah routerboard dengan satu IP public. Pengujian dilakukan dengan analisa proses pemilihan jalur routing, analisa kecepatan waktu convergence , analisa kecepatan update routing dan pengujian pengiriman paket pada masing-masing router. Metode yang digunakan adalah studi literatur, simulasi pada virtualbox, dan implementasi pada jaringan test-bed. Hasil tes waktu convergence menggunkan ISP yang sama adalah 55,28 detik dan menggunkan ISP yang berbeda adalah 55,13 detik. Hasil pengujian pada proses routing update dengan ISP yang sama adalah 7,23 detik dan 9,63 detik menggunakan ISP yang berbeda. Secara keseluruhan routing OSPF pada jaringan Open VPN mampu bekerja dengan baik dengan waktu convergence dan waktu update routing yang cepat dan up to date.

Kata kunci : *Routing, OSPF*, Open VPN

PENDAHULUAN

Teknologi informasi khususnya jaringan komputer berkembang dengan sangat pesat seiring dengan kebutuhan masyarakat akan layanan yang memanfaatkan jaringan komputer. Hal ini bisa di lihat semakin banyaknya organisasi dan perusahaan yang menggunakan jaringan komputer untuk melancarkan arus informasi didalam perusahaan tersebut.Komunikasi antara kantor cabang dan kantor pusat dibutuhkan media transmisi sebagai sarana kumunikasi data, untuk membangun jaringan dalam satu kota bisa menggunakan media *wireless* atau kabel untuk menghubungkan antara kantor satu dan kantor lainnya. VPN bisa dipakai sebagai cara alternatif untuk menghubungkan jaringan lokal yang cukup luas dengan biaya yang lebih rendah. Karena transmisi data yang digunakan pada VPN memakai media jaringan *internet* atau jaringan publik yang sebelumnya telah ada tanpa perlu membangun jaringan sendiri. Dalam penelitian ini penulis menggunakan salah satu tipe VPN yaitu Open VPN. Kelebihan

Open VPN adalah menggunakan algoritma *sha1* dan *md5* untuk proses autentikasi, dan menggunakan beberapa *chiper* yaitu *blowfish128, aes128, aes192* dan *aes256*.

Jaringan antar kantor terdapat banyak *router* yang harus terhubung satu sama lain, *Protocol routing* yang digunakan dalam penelitian ini adalah OSPF (*Open Shortest Path First).* Manfaat routing OSPF, meminimalisir routing table, meminimalisir perubahan topologi, agar perubahan topologi hanya berdampak disatu area, dan jaringan dibagi-bagi menjadi beberapa kelompok area yang dibuat bertingkat, sehingga penyebaran informasi lebih teratur dan tersegmentasi, sehingga penggunaan *bandwidth* jaringan menjadi lebih baik, lebih cepat mencapai *convergence*, dan lebih akurat dalam menentukan rute-rute terbaik menuju kesebuah lokasi. Berdasarkan uraian latar belakang masalah yang telah dipaparkan di atas maka muncul gagasan untuk membuat implementasi *routing* OSPF melalui jaringan Open VPN. Yang bertujuan membangun jaringan menggunakan Open VPN pada mikrotik di kantor pusat dan kantor cabang, implemntasi *routing* OSPF pada mikrotik untuk menghubungkan *router* kantor pusat dan kantor cabang, dan menganalisa kinerja *routing* OSPF pada jaringan Open VPN.

TINJAUAN PUSTAKA

Syafrudin (2010), melakukan penelitian berupa analisa kinerja dari *routing protocol* pada jaringan IPv6 yaitu RIPng dan OSPFv3. Pengujian dilakukan dengan analisa proses pemilihan jalur pada *routing table*, analisa paket header, dan pengujian dengan melakukan pengiriman paket pada masing-masing *routing protocol* . Metode yang digunakan adalah studi literatur, simulasi pada komputer, dan implementasi pada jaringan *test-bed*. Hasilnya adalah analisa data menunjukan bahwa secara umum kinerja RIPng dan OSPFv3 tidak jauh berbeda dengan *routing protocol* pendahulunya, yaitu RIP dan OSPF pada jaringan IPv4, perbedaan mendasar adalah dukungan terhadap pengalamatan 128-bit. Pada pengujian didapatkan kinerja OSPFv3 lebih baik karena kecepatannya dalam melakukan *convergence* pada jaringan ketika terjadi *link down* dibutuhkan waktu sebesar 4,542 detik, jaluh lebih cepat dari pada RIPng yang membutuhkan waktu 60,566 detik.

Wahyudi (2011), membuat implementasi *Virtual Private Network* (VPN) server menggunakan Slackware 13 untuk keamanan komunikasi data pada PT. Time Exelindo ISP. Penelitian tersebut membahas analisis dan merancang infrastruktur jaringan *Virtual Private Network* (VPN) menggunakan Open VPN serta menganalisis kualitas data dan *trafficc* pada jaringan open VPN. Hasilnya adalah OpenVPN dapat digunakan untuk melindungi data-data sensitif yang dikirim maupun diterima konsumen melalui internet

Caesar (2014), membuat penerapan *Virtual Private Network* (VPN) menggunakan mikrotik router pada RS Immanuel Bandung. Penelitian tersebut menggunakan PPTP (*Point To Point unnel Protocol)* pada Mikrotik untuk mengelola jaringan yang kompleks dengan biaya yang relatif sangat murah. Hasilnya adalah *remote access Virtual Private Network* (VPN) membantu administrator jaringan dalam melakukan maintenance dan perbaikan jaringan.

Berdasarkan penelitian-penelitian yang telah dilakukan sebelumnya, maka penulis melakukan penelitian analisis kinerja *routing* OSPF pada jaringan Open VPN yang menggabungkan antara *routing* OSPF dengan teknologi Open VPN yang berada pada referensi sebelumnya. Selain analisis tersebut, penulis juga mengimplementasikan *routing* OSPF pada jaringan Open VPN menggunakan mikrotik.

1. Virtual Private Network (VPN)

   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, tetapi terdiri dari paket diarahkan melalui variasi mesin diinternet secara *ad-hoc*. Koneksi *virtual* yang aman yang dibuat antara dua mesin, mesin dan jaringan, atau dua jaringan. (Wahyudi, 2011)

   Menurut IETF, *Internet Engineering Task Force* VPN merupakan suatu bentuk private internet yang melalui public *network* (*internet*), dengan menekankan pada keamanan data dan akses global melalui internet. Hubungan ini dibangun melalui suatu *tunnel* (terowongan) virtual antara dua node.Data *dienkapsulasi* (dibungkus) dengan header yang berisi informasi *routing* untuk mendapatkan koneksi *point to point* sehingga data melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan

untuk mendapatkan koneksi yang bersifat private, data harus *dienkripsi* terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses *dekripsi*. Proses *enkapsulasi* data sering disebut *tunneling.*

2. Routing

Routing adalah proses penentuan jalur terbaiak (*best path)* untuk mencapai suatu *network* tujuan. *Routing* juga dapat berarti proses memindahkan paket data dari host pengirim ke host tujuan dimana host pengirim dan host tujuan tidak berada dalam satu *network*. (Towidjojo, 2012)

Dalam melakukan *routing* , *router* akan menyimpan berbagai informasi *routing* sehingga dapat menentukan kemana sebuah paket akan dikirimkan. Informasi *routing* ini memuat jalur terbaik (*best path)* yang sebaiknya ditempuh oleh sebuah paket. Informasi *routing* disimpan oleh *router* pada sebuah tabel yang di sebut tabel *routing* .

Didalam tabel *routing* informasi *routing* akan disimpan bentuk *entry-entry route*. Setiap *entry route* akan menunjukan *network* address dari *network* yang dapat dituju oleh *router* tersebut dan berisi tentang informasi bagaimana cara mencapai *network* tersebut.

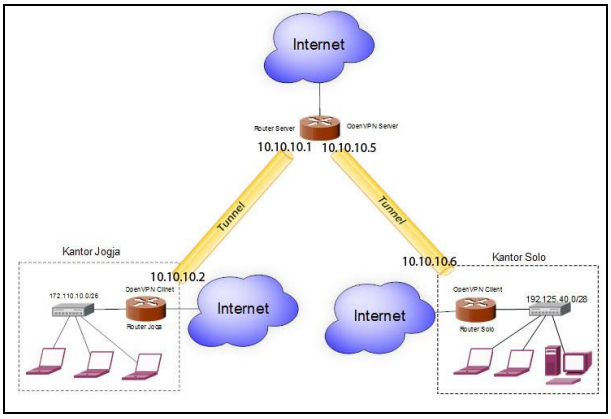
3. OSPF (Open Shortest Part First)

OSPF (*Open Shortest Path First*) merpakan *routing protocol link state* dan digunakan untuk menghubungkan *router-router* yang berada dalam satu *Autonomous System* (AS) sehingga *routing protocol* ini termasuk juga katagori *Interior Gateway Protocol* (IGP). Autonomous system itu sendiri merupakan kumpulan *router-router* yang berada dibawah kendalai administrasi dan strategi *routing* yang sama. (Towidjojo, 2013)

OSPF diterapkan pada jaringan skala besar karena memiliki kemampuan untuk mencapai kondisi *convergence* yang sangat cepat, baik pada saat jaringan pertama dihidupkan maupun bila terjadi perubahan jaringan.

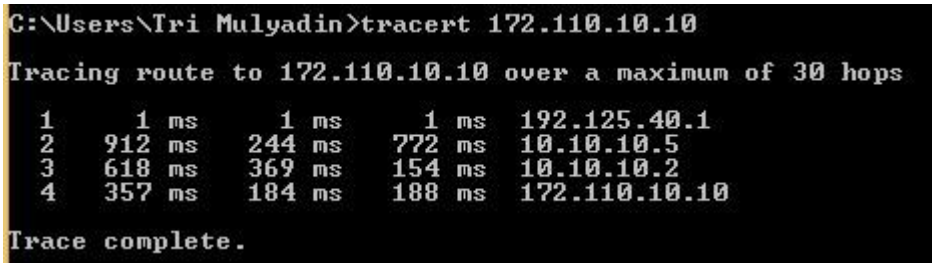
PEMBAHASAN

Topologi yang dipakai dalam penelitian ini dapat dilihat pada Gambar 1, disitu terdapat tiga buah router terdapat tiga kantor yang berbeda kota yang dihubungkan dengan *tunnel* Open VPN melalui media internet. Dalam hal ini, setiap router yang berada di kantor cabang di fungsikan sebagai Open VPN client dan dihubungkan ke Open VPN server pada router kantor pusat. Open VPN client akan *dial-up* ke IP *public* yang terdapat di router server, kemudian server akan memberikan IP address untuk client yang berfungsi menghubungkan jaringan melaui internet. Selanjutnya supaya jaringan lokal antar kantor bisa saling berhubungan, dibutuhkan teknik *routing* untuk menghubungkan jaringan yang berbeda *network* agar bisa bertukar data dan informasi. Pada implementasi digunakan *routing* OSPF melalui Open VPN yang diharapkan mampu menghubungkan jaringan pada ketiga kantor tersebut meskipun jaringan berbeda *network* dan lokasi.



Gambar 1. Topologi Jaringan

Setelah semua router dan user telah dikonfigurasi, dilakukan pengujian Analisa jalur routing, analisa waktu *convergence,* analisa waktu update routing, analisa *hroughput*, delay dan packet loss. Pengujian analisa jalur routing dilakukan dengan *trace route* pada PC kantor Solo menuju PC kantor Jogja yaitu dengan printah "tracert 172.110.10.10". Dengan perintah *traceroute* dapat diketahui *interface-interface* dan *router* yang dilalui paket untuk mencapai tujuan.

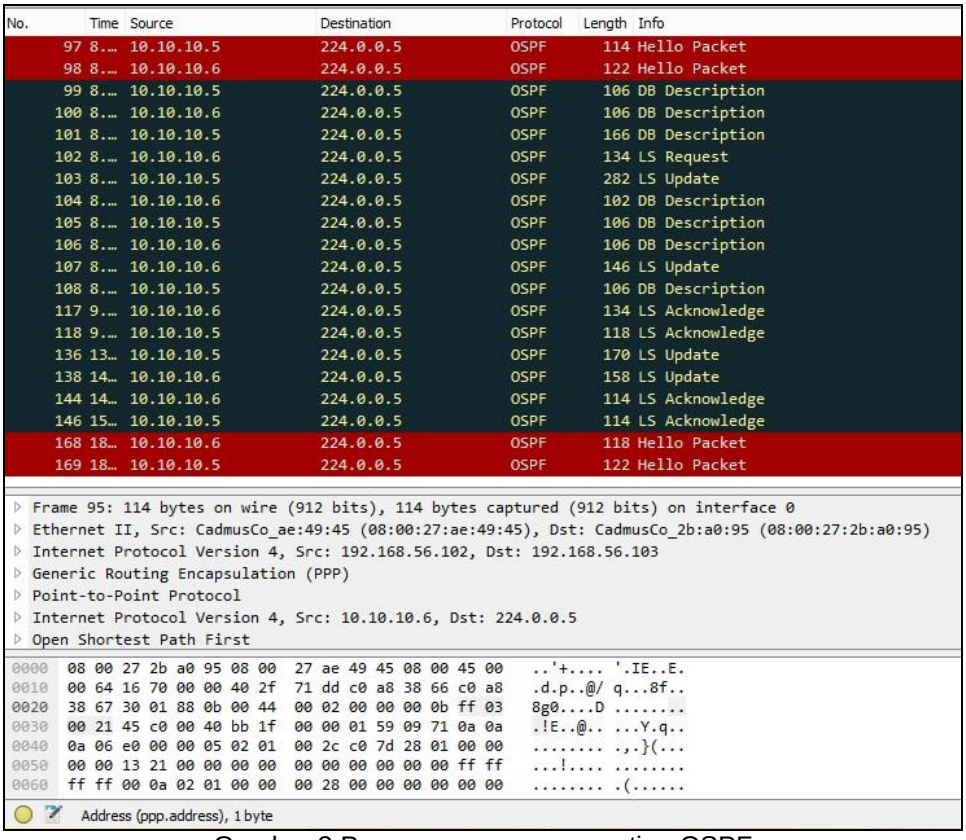


Gambar 2. Hasil Traceroute

Dari Gambar 2 diketahui, bahwa jalur *routing* yang dilalui dari PC Solo ke PC Jogja diawali masuk ke *router* Solo melalui *gateway* 192.125.40.1 pada *router* Solo, diteruskan ke *router server* melalui *gateway* 10.10.10.5, selanjutnya di teruskan ke *router* Jogja melalui *gateway* 10.10.10.2 dan terakhir diterukan ke *network* lokal yang berada dibawah *router* Jogja.

Pengujian waktu convergence dilakukan dilakukan dengan melakukan pemutusan *network* Open VPN,sedangakan pengujian kecepatan *update routing* adalah dengan memutuskan salah satu *interface* yang aktif pada salah satu *router. Router* yang menjalankan *routing* OSPF hanya akan bertukar informasi tabel *routing* dengan *router* yang menjalankan *routing* OSPF lainnya yang berada dalam satu *Autonomous System* (AS). Pada *routing* OSPF dikenal kondisi *adjacency* antar *router*. Sebelum *router-router* bertukar tabel *routing*, maka sebuah *router* harus terlebih dahulu mencapai kondisi *adjacency* dengan *router* tetangganya. Setelah mencapai kondisi *adjacency* antara satu *router* dengan lainnya, maka *router* tersebut akan berusaha mewujudkan *network* yang *convergence*. *Network* yang *convergence* adalah *network* dimana *router-router* di dalamnya telah memiliki tabel *routing* yang akurat dan *up to date.*

Pengujian dilakukan pada saat traffic jaringan sepi yaitu pada saat jaringan internet jarang digunakan pada pukul jam 12 malam sampai jam 7 pagi dan pada saat traffic jaringan sedang padat yaitu pada saat jaringan internat banyak digunakan yaitu pada saat jam sibuk bekerja pada jam 7 pagi sampai jam 5 sore, selain itu pengujian juga dilakukan dengan menggunakan ISP (Internet Service Provider) yang sama dan ISP yang berbeda atara client dan server Open VPN. Paket yang digunakan dalam pengujian adalah 20 paket ping, dengan panjang data 32 *byte*. Untuk mengetahui proses untuk mencapai kondisi *convergence* yang ditunjukan pada Gambar 3.



Gambar 3 Proses convergence routing OSPF

Dalam proses convergence routing OSPF ada beberpa tahap yang harus dilalui, dari Gambar 3 bisa dilihat bagaimana proses convergence itu tejadi, berikut penjelasan dari Gambar 3 hasil capture menggunakan software wireshark:

1. Setelah jalur Open VPN terhubung, setiap *router* kan mengirimkan *Hello packet* ke *router* tetangganya secara *multicast dengan menggunakan IP address* tujuan 224.0.0.5.
2. Setiap router akan menerima *Hello packet* dari tetangganya, sehingga pada tahap ini kondisi *adjacency* sudah tercapai.
3. Ketika kondisi *adjacency* sudah tercapai, setiap *router* akan membuat *DBD packet* yang berisi *Link state Database* yang akan dikirimkan ke *router* tetangganya.
4. Setiap *router* akan menerima *DBD packet*, kemudian akan membandingkan dengan *Link State Database* yang dimilikinya untuk kemudian disinkronkan.
5. *Selanjutnya router* akan mebuat *Link State Request packet* bertujuan meminta informasi yang ada dalam *Link State Database* milik *router* tetangganya.
6. *Kemudian router* tujuan akan membuat *Link State Update packet* sebagai jawaban dari *Link State Request packet* yang berisi informasi tabel *routing* dari setiap *router*.
7. Terakhir adalah *router* membuat *Link State Acknowledge packet* yang bertujuan untuk memberitahukan kepada *router* pengirim *Link State Update packet* bahwa *Link State Update packet* telah diterima.
8. Sampai tahap ini proses menuju *convergence* telah selesai, sehingga masing-masing *router* telah memiliki tabel *routing* yang sama dengan yang lainnya.
9. *Hello packet* akan tetap dikirimkan setiap *router* meskipun kondisi *convergence* telah tercapai, tujuannya untuk menjaga tabel *routing* yang akurat dan *up to date. Hello packet* dikirim setiap 10 detik, tergantung pengaturan pada masing-masng *router*.

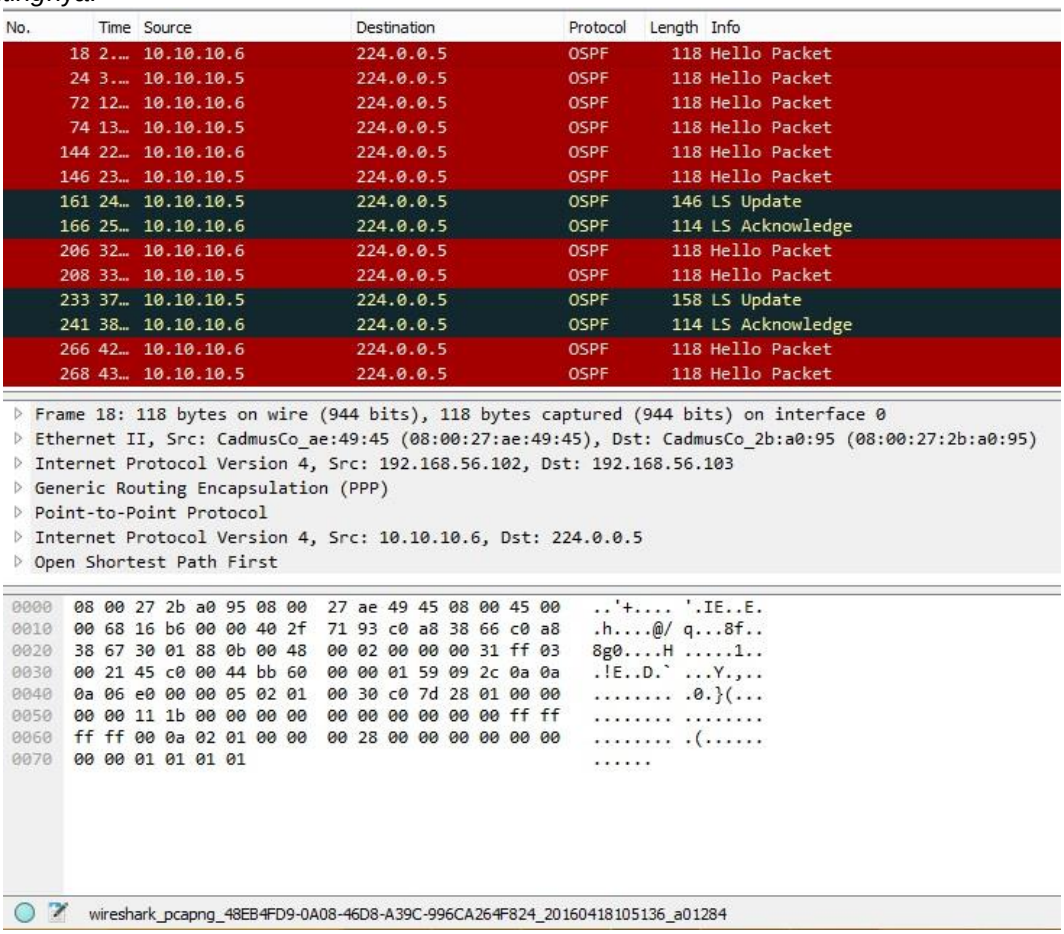
Hasil Proses pengujian, untuk mencapai kondisi *convergence* pada jaringan Open VPN yang telah dibangun, diperlukan rata-rata waktu 55,13 detik pada saat jaringan sepi dan diperlukan rata-rata waktu 72,80 detik pada saat jaringan sedang padat dengan menggunakan ISP yang berbeda dan diperlukan rata-rata waktu 55,28 detik pada saat jaringan sepi dan diperlukan rata-rata waktu 55,98 detik pada saat jaringan sedang padat dengan menggunakan

ISP yang sama. Perbedaan waktu *convergence* dengan menggunakan ISP yang berbeda dan ISP yang sama adalah 0,15 detik pada saat jaringan sedang sepi dan 16,82 detik pada saat jaringan sedang padat. Dari hasil pengujian kecepatan waktu *convergence* dengan menggunakan ISP yang sama lebih cepat dari yang menggunakan ISP yang berbeda.

Proses update routing berbeda dengan proses convergence, dimana dalam proses mencapai *convergence* sebelumnya harus mencapai kondisi *adjacency* terlebih dahulu. Dalam proses *update routing*, kondisi *adjacency* dan *convergence* telah tercapai. Ketika pada salah satu *router* terdapat *link* yang *down* atau *interface* mengalami kerusakan, *router* akan memberitahukan kepada *router* tetanganya bahwa terdapat *link* yang mati atau *down.* Selain itu *update routing* juga terjadi bila ada *link* atau *interface* yang tadinya *down* menjadi hidup kembali, sehingga *router* akan memberitahukan kepada *router* tetangganya bahwa *link* sudah hidup kembali.

Pada Gambar 4 terjadi proses *update routing* pada pengujian memutuskan *link* yang aktif disalah satu *router* dan menghidupkannya kembali. Pada baris nomor 161 terdapat *Link State Update packet* dari salah satu *router* yang memberitahukan bahwa terdapat *link* yang *down*, dibaris nomor 166 *router* membuat *Link State Acknowledge packet* yang bertujuan untuk memberitahukan kepada *router* pengirim *Link State Update packet* bahwa *Link State Update packet* telah diterima dan *router* tersebut menghapus *network* dari *link* yang *down* pada tabel *routing*nya.

Pengujian selanjutnya mengaktifkan kembali *link* yang sebelumnya telah *down*. Pada baris nomor 233 *router* mengirim *Link State Update packet* untuk memberitahukan bahwa *link* sudah hidup kembali, di baris nomor 241 *router* membuat *Link State Acknowledge packet* yang bertujuan untuk memberitahukan kepada *router* pengirim *Link State Update packet* bahwa *Link State Update packet* telah diterima dan memasukan *network* yang barusan hidup dalam tabel *routing*nya.



Gambar 4 Proses update routing OSPF

Dari pengujian, dibutuhkan rata-rata waktu untuk *update routing* ketika terdapat *link* yang *down* adalah 4,77 detik pada saat jaringan sepi dan pada saat jaringan padat dibutuhkan rata-rata waktu 4,86 detik dengan menggunakan ISP yang berbeda dan diperlukan rata-rata waktu 2,19 detik pada saat jaringan sepi dan diperlukan rata-rata waktu 5,04 detik pada saat jaringan sedang padat dengan menggunakan ISP yang berbeda**.** Kemudian rata-rata waktu untuk *update routing* ketika *link* yang *down* sudah hidup kembali adalah 6,17 detik pada saat jaringan sepi dan pada saat jaringan padat dibutuhkan rata-rata waktu 9,58 detik dan diperlukan rata-rata waktu 2,16 detik pada saat jaringan sepi dan diperlukan rata-rata waktu 2,73 detik pada saat jaringan sedang padat dengan menggunakan ISP yang berbeda. Perbedaan waktu *update routing* ketika *link down* dengan menggunakan ISP yang berbeda dan ISP yang sama adalah 2,58 detik pada saat jaringan sepi dan 0,18 detik pada jaringan sedang padat, selanjut perbedaan waktu *update routing* ketika *link down* sudah hidup kembali adalah 4,01 detik pada jaringan sedang sepi dan 6,85 detik pada saat jaringan sedang padat**.** Dari hasil pengujian kecepatan update routing dengan menggunakan ISP yang sama lebih cepat dari yang menggunakan ISP yang berbeda.

Pengujian pengukuran *throughput* dari PC kantor Solo kepada PC kantor Jogja menggunakan *Software Axence Nettools,* pengujian dilakukan selama 5 menit sebanyak 5 kali, pada saat jaringan sedang sepi didapat rata-rata *throughput* 9495,2 *Byte/second* dan pada saat jaringan sedang padat didapat rata-rata *throughput* 6250,2 *Byte/second* dengan besar *packet* 1000 *Byte* menggunakan ISP yang berbeda*,* dan didapat rata-rata *throughput* 19066,6 *Byte/second* pada saat jaringan sepi dan pada saat jaringan sedang padat didapat rata-rata *throughput* 18225,8 *Byte/second* dengan besar *packet* 1000 *Byte* menggunkan ISP yang sama*.*

Pengujian pengukuran *delay* dari PC kantor Solo kepada PC kantor Jogja menggunakan *Software Axence Nettools,* pengujian dilakukan selama 5 menit sebanyak 5 kali, pada saat jaringan sedang sepi didapat rata-rata 181 ms dan pada saat jaringan sedang padat didapat rata-rata 397 ms menggunakan ISP yang berbeda, dan didapat rata-rata 79,8 ms pada saat jaringan sepi dan pada saat jaringan sedang padat didapat rata-rata 288 ms menggunakan ISP yang sama. Menurut versi TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) standarisari nilai *delay* sebagai berikut.

Tabel 1. Standarisasi delay versi TIPHON

Kategori delay	**Besar delay**
Sangat bagus	< 150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	>450 ms

Mengacu pada Tabel 1mengenai standarisasi *delay* versi TIPHON, hasil pengujian *delay* pada saat jaringan sepi dengan ISP yang berbeda masuk kategori Bagus dan pada saat jaringan padat masuk kategori sedang, hasil pengujian *delay* pada saat jaringan sepi dengan ISP yang sama masuk kategori Sangat bagus dan pada saat jaringan padat masuk kategori Bagus. Pengujian pengukuran *packet loss* dari PC kantor Solo kepada PC kantor Jogja menggunakan *Software Axence Nettools,* pengujian dilakukan selama 5 menit sebanyak 5 kali, pada saat kondisi jaringan sepi didapat rata-rata 0 % dan pada saat kondisi jaringan padat didapat rata-rata 13,6 % dengan menggunakan ISP yang berbeda, dan didapat rata-rata 1 % dan pada saat kondisi jaringan padat didapat rata-rata 1,3 % dengan menggunakan ISP yang sama. Menurut versi TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) standarisari nilai *packet loss* sebagai berikut.

Tabel 2. Standarisasi packet loss versi TIPHON

Kategori packet loss	**Packet loss**
Sangat bagus	0%
Bagus	3 %
Sedang	15%
Jelek	25%

Mengacu pada Tabel 2 mengenai standarisasi *packet loss* versi TIPHON, hasil pengujian *packet loss* pada saat kondisi jaringan sepi masuk kategori Sangat bagus dan pada saat kondisi jaringan padat masuk kategori sedang dengan menggunakan ISP yang berbeda, hasil pengujian *packet loss* pada saat kondisi jaringan sepi masuk kategori Sangat bagus dan pada saat kondisi jaringan padat masuk kategori sangat bagus dengan menggunakan ISP yang sama.

Pada implementasi dan pengujian menggunakan ISP (Internet Service Provider) yang berbeda dan ISP yang sama. Dari hasil analisis sangan mempengaruhi dalam kinerja jaringan seperti, kecepatan waktu *convergence, update routing,* dan QoS. Hal ini disebabkan *route* yang dilewati untuk mencapai tujuan, apakah banyak melewati router atau sedikit melewati router. Hasil *traceroute* akan membuktikan berapa router yang harus dilewati untuk mencapai tujuan. Pada Gambar 5 menunjukan hasil *traceroute* menggunkan ISP yang sama dan Gambar 6 menggunakan ISP yang berbeda.

```
C:\Users\Tri Mulyadin>tracert 180.246.179.115

Tracing route to 180.246.179.115 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  1.10.110.172.in-addr.arpa [172.110.10.1]
  2     2 ms     3 ms     1 ms  1.100.168.192.in-addr.arpa [192.168.100.1]
  3     3 ms     4 ms     2 ms  36.79.128.1
  4   174 ms   173 ms   168 ms  180.246.179.115

Trace complete.
```

Gambar 5 Hasil traceroute ISP yang sama

```
C:\Users\Tri Mulyadin>tracert 202.169.232.170

Tracing route to host-202-169-232-170.jogjamedianet.com [202.169.232.170]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  172.110.10.1
  2     1 ms     1 ms     1 ms  192.168.100.1
  3     3 ms     2 ms     3 ms  36.79.128.1
  4    14 ms     3 ms     5 ms  125.160.15.57
  5    12 ms     2 ms     6 ms  61.94.114.121
  6    13 ms    12 ms    12 ms  109.subnet118-98-51.astinet.telkom.net.id [118.9
8.51.109]
  7    15 ms    13 ms    13 ms  110.subnet118-98-51.astinet.telkom.net.id [118.9
8.51.110]
  8    27 ms    22 ms    22 ms  118.97.5.93
  9    23 ms    23 ms    22 ms  118.97.5.94
 10    23 ms    23 ms    22 ms  host-202-169-224-14.jogjamedianet.com [202.169.2
24.14]
 11    29 ms    23 ms    24 ms  ubr7246vxr.jogjamedianet.com [202.169.224.48]
 12    34 ms    32 ms    47 ms  host-202-169-232-170.jogjamedianet.com [202.169.
232.170]

Trace complete.
```

Gambar 6 Hasil traceroute ISP yang berbeda

Hasil dari *traceroute* membuktikan, bahwa dengan menggunakan ISP yang sama melewati 4 *hops* dan yang menggunakan ISP yang berbeda harus melewati 12 *hops* untuk mencapai tujuan. Hal ini membuktikan dengan menggunkan ISP yang sama dapat lebih cepat mencapai tujuan dari pada menggukan ISP yang berbeda yang banyak melawati *hops* sehingga memperlambat dalam perjalanan menuju tujuan.

KESIMPULAN

1. Menggunakan ISP yang berbeda kecepatan *convergence* diperlukan rata-rata waktu 55,13 detik pada saat jaringan sepi dan diperlukan rata-rata waktu 72,80 detik pada saat jaringan padat. kecepatan *update routing* ketika terjadi *link down* dibutuhkan rata-rata 4,77 detik pada saat jaringan sepi dan pada saat jaringan padat dibutuhkan rata-rata waktu 4,86 detik, dan dibutuhkan 6,17 detik pada saat jaringan sepi dan pada saat jaringan padat dibutuhkan rata-rata waktu 9,58 detik untuk *update routing* ketika *link* yang *down* hidup kembali
2. Menggunakan ISP yang sama kecepatan *convergence* diperlukan rata-rata waktu 55,28 detik pada saat jaringan sepi dan diperlukan rata-rata waktu 55,98 detik pada saat

jaringan padat. Pada pengujian kecepatan *update routing* ketika terjadi *link down* dibutuhkan rata-rata 2,19 detik pada saat jaringan sepi dan pada saat jaringan padat dibutuhkan rata-rata waktu 5,04 detik, dan dibutuhkan 2,16 detik pada saat jaringan sepi dan pada saat jaringan padat dibutuhkan rata-rata waktu 2,72 detik untuk *update routing* ketika *link* yang *down* hidup kembali.

3. Menggunakan ISP yang sama dalam membangun jaringan Open VPN dapat mempercepat kinerja jaringan, karena *route* yang dilewati sedikit sehingga cepat mencapai tujuan.
4. Secara keseluruhan routing OSPF pada jaringan Open VPN mampu bekerja dengan baik dengan kecepatan waktu *convergence* dan kecepatan waktu update routing yang cepat baik pada saat jaringan sedang sepi maupun jaringan sedang padat.

DAFTAR PUSTAKA

Caesar, Y., 2014, *Penerapan Virtual Private Network Menggunakan Mikrotik Router Pada RS Immanuel Bandung,* Skripsi, Jurusan Sistem Informasi, STIMIK LPKIA, Bandung

Syafrudin, M., 2010, *Analisa unjuk kerja routing protocol RIPng dan OSPFv3 pada jaringan IPv6,* Skripsi, Jurusan Teknik Elektro, FT, Universitas Indonesia, Depok

Towidjojo, R., 2013, *Konsep & Implementasi Routing Dengan Router Mikrotik 200% Connected, Jasakom*, Jakarta

Wahyudi, D. A., 2011, *Implementasi Virtual Private Network Server Menggunakan Slackware 13 Untuk Keamanan Komunikasi Data (Studi kasus : PT. Time Exelindo ISP),*Skripsi, Jurusan Teknik Informatika, STIMIK AMIKOM, Yogyakarta.