



Performa Protokol Routing OSPF dan BGP pada Jaringan VOIP MPLS dengan Tunelling L2TP/IPSec

Bekti Maryuni Susanto, Ery Setiyawan Jullev Atmaji

*#Jurusan Teknologi Informasi Politeknik Negeri Jember
Jl. Mastrip Kotak Pos 164 Jember*

bekti@polije.ac.id

ery@polije.ac.id

Abstract

Voice communication can be achieved through IP-based networks, be it Internet, Intranet or Local Area Network. Multiprotocol label switching (MPLS) is a convergence of connection-oriented forwarding techniques and Internet routing protocols. This paper discusses the performance of OSPF routing protocols on MPLS VPN-based VOIP networks. The routing protocol applied to this research is Open Shortest Path First (OSPF). The VPN used in this research is L2TP / IPSec. MPLS VPN network is built using three LSR routers and two LER routers. The LSR router is responsible for carrying out packet forwarding while the LER router is responsible for adding or removing labels on packets that go to or leave the MPLS domain. L2TP / IPSec is responsible for securing VOIP communication channels by tuning. Evaluation is done by measuring the quality of VOIP service either without using MPLS or by using MPLS VPN. Based on the research results can be concluded that with the application of VPN on MPLS network able to improve the security of communication channel on VoIP network.

Keywords— VOIP, MPLS, VPN, L2TP/IPSec.

I. PENDAHULUAN

Peningkatan jumlah pengguna Internet membuat layanan seperti telepon mencapai pelanggan mereka melalui Internet atau yang sering disebut dengan Voice over Internet Protocol (VoIP). Komunikasi suara dapat dicapai melalui jaringan berbasis IP, baik itu Internet, Intranet maupun Local Area Network (LAN) [1]. Hal ini membuat Internet Service Provider (ISP) untuk meningkatkan kualitas layanan mereka. Dengan peningkatan ini, router tradisional mengalami tantangan untuk menyediakan bandwidth tinggi yang dibutuhkan, fast routing serta dukungan kualitas layanan (QoS). Sehubungan dengan tantangan router tradisional untuk menyediakan permintaan ini khususnya untuk suara dan video, maka digunakan metode Multi Protocol Label Switching (MPLS) [2]. MPLS mampu meningkatkan kinerja router dalam memberikan layanan yang bersifat real time [3]. Multiprotocol label switching (MPLS) adalah sebuah konvergensi teknik forwarding connection-oriented dan protokol routing Internet. Inkarnasi standar MPLS yang paling menonjol memanfaatkan kemampuan peralihan sel berkinerja tinggi dari perangkat switch switch asinkron (ATM), dan menyatukannya menjadi jaringan yang menggunakan protokol routing IP yang ada [4]. Seiring kemajuan standardisasi, MPLS berbasis paket

juga muncul untuk menyederhanakan mekanisme pemrosesan paket di dalam router inti, menggantikan klasifikasi header penuh atau sebagian dan pencarian terpanjang prefiks dengan pencarian indeks label sederhana.

Teknik yang umum digunakan di antara ISP besar adalah menggunakan jaringan lapisan 2 (ATM atau FR) untuk mengelola jaringan. Dalam pendekatan ini sering disebut solusi overlay, rangkaian lengkap sirkuit virtual yang menghubungkan backbone IP. Ini berfungsi untuk mencegah agregasi yang terjadi pada routing hop-by hop di backbone IP dengan routing berbasis tujuan. Dalam pendekatan ini, arus dapat dirutekan secara individual melalui topologi lapisan 2 dan traffic engineering dapat dicapai. Tapi kelemahan pendekatan ini adalah masalah skalabilitas dan bahwa satu kegagalan link dapat menyebabkan puluhan Virtual Circuits turun, memaksa protokol perutean IP untuk dikonversi kembali. Solusi untuk masalah ini bisa dilakukan koordinasi antara layer 2 network dan layer 3 IP network. Solusi ini adalah MPLS, seperangkat prosedur untuk menggabungkan kinerja, QoS dan manajemen traffic dari paradigma label-swapping Layer 2 dengan skalabilitas dan fleksibilitas fungsi routing Layer 3 [5].

VOIP menggunakan routing konvensional memiliki kualitas panggilan yang rendah sehubungan adanya delay

dan paket loss. Untuk mengirimkan lalu lintas real time melalui jaringan data menjadi tantangan besar bagi peneliti. MPLS adalah solusi terbaik untuk meningkatkan kualitas layanan VOIP. MPLS adalah solusi terbaik untuk meningkatkan kualitas layanan VOIP. MPLS memiliki beberapa alasan untuk menjadi protokol masa depan [5]. Pertama, MPLS benar-benar memiliki arsitektur yang multiprotokol. Dimana MPLS memanfaatkan mekanisme switching menggunakan label yang sederhana yang sangat fleksibel pada aplikasi yang telah ada, misal MPLS pada ATM dan frame relay. Kedua, melalui pemanfaatan classification, queue and scheduling (CQS) traffic engineering, MPLS mampu melakukan pengendalian fitur-fitur kualitas layanan. Ketiga, MPLS menyediakan solusi skalabilitas dan memungkinkan fleksibilitas yang signifikan di dalam routing. Keempat, arsitektur connection oriented dan fitur kualitas layanan yang dapat dipercaya dengan mudah memungkinkan fitur layanan end user dengan kualitas tinggi.

Paper ini membahas tentang performa protokol routing OSPF pada jaringan VOIP berbasis MPLS VPN. Protokol routing yang diterapkan pada penelitian ini, yaitu Open Shortest Path First (OSPF). VPN yang digunakan adalah L2TP/IPSec. Evaluasi dilakukan dengan mengukur kualitas layanan baik menggunakan MPLS VPN maupun tanpa menggunakan MPLS. Pengukuran dilakukan terhadap throughput, delay, packet loss dan jitter. Simulasi jaringan VOIP berbasis MPLS VPN menggunakan software GNS3 dan Oracle Virtual Box. GNS3 digunakan untuk membuat model topologi jaringan sedangkan Virtual Box digunakan untuk menjalankan VOIP Server dan komputer klien.

II. TUJUAN DAN MANFAAT PENELITIAN

A. Tujuan Penelitian

1. Melakukan analisis topologi jaringan VoIP MPLS berbasis VPN dengan tunneling L2TP/IPSec.
2. Melakukan analisis Quality of Service (QoS) VoIP pada jaringan Multi Protocol Label Switching (MPLS) berbasis VPN dengan tunneling L2TP/IPSec.
3. Melakukan Analisis tingkat keamanan VoIP pada jaringan Multi Protocol Label Switching (MPLS) berbasis VPN dengan tunneling L2TP/IPSec.

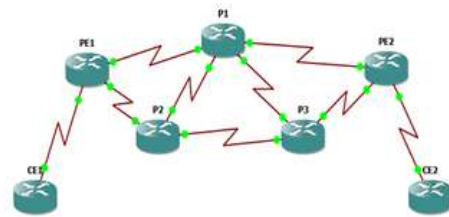
B. Manfaat Penelitian

1. Pemanfaatan VoIP menjadikan biaya komunikasi lebih murah dan jaringan lebih sederhana.
2. Pemeliharaan jaringan lebih murah karena jaringan komunikasi menjadi satu dengan jaringan komputer.
3. Pemanfaatan VPN pada jaringan VoIP menjadikan VoIP lebih aman tidak mudah dilakukan penyadapan.
4. Pemanfaatan MPLS pada jaringan VoIP menjadikan QoS lebih baik dibandingkan dengan tanpa menggunakan MPLS.

III. METODE PENELITIAN

Penelitian ini mengimplementasikan protokol routing OSPF pada jaringan VOIP berbasis MPLS VPN. Protokol routing yang digunakan pada penelitian ini adalah *open shortest path first* (OSPF). Jaringan MPLS VPN dibangun dengan menggunakan tiga buah router LSR dan dua buah router LER. Router LSR bertanggungjawab dalam melakukan packet forwarding sedangkan router LER bertanggungjawab dalam menambah atau menghapus label pada packet yang menuju atau meninggalkan domain MPLS. L2TP/IPSec bertanggungjawab dalam mengamankan saluran komunikasi VOIP dengan melakukan tunneling..

Pada Gambar 1 terdapat lima buah router yang berfungsi untuk melakukan forwarding MPLS routing dan melakukan switching traffic di dalam jaringan di bawah domain administratif tunggal. Pada MPLS terdapat dua peran utama yaitu *Label Switch Router* (LSR) dan *Label Edge Router* (LER) [6]. LSR bertanggung jawab untuk melakukan forwarding paket sesuai label switching dan router ini terletak di inti dari jaringan MPLS. Pada penelitian ini menggunakan tiga buah LSR yaitu Router P1, P2, dan P3. LSR mempunyai kemampuan untuk melakukan routing paket layer 3. Sedangkan LER bertanggung jawab menambah atau menghapus label paket yang menuju atau keluar dari router LER tersebut[10]. LER mempunyai kemampuan untuk melengkapi routing paket layer 3. Pada penelitian digunakan dua buah LER yaitu Router PE1 dan Router PE2. Sedangkan router CE1 dan Router CE2 adalah router yang berhubungan langsung dengan user. User pada topologi ini terdapat dua user yang menjalankan aplikasi telepon berbasis Internet dan L2TP/IPSec Client. VOIP server terhubung dengan salah satu router LSR dan menjalankan layanan L2TP/IPSec Server.



Gambar 1. Desain topologi jaringan VOIP berbasis MPLS VPN

Evaluasi penerapan protokol routing OSPF pada jaringan VoIP berbasis MPLS VPN dilakukan dengan mengukur Quality of Service yang terdiri dari throughput, delay, packet loss dan jitter. Pengukuran dilakukan dengan mengamati paket RTP menggunakan software wireshark. Dari hasil pengukuran selanjutnya hasil QoS dibandingkan baik saat menggunakan jaringan MPLS VPN maupun tanpa menggunakan jaringan MPLS.

IV. HASIL DAN LUARAN YANG DICAPAI

A. Hasil Penelitian

Eksperimen dilakukan dengan membangun jaringan VOIP berbasis MPLS VPN. Router yang digunakan berjumlah tujuh buah router yang terdiri dari 3 router LSR, 2 router LER dan 2 router CE. Router LSR bertanggung jawab dalam melakukan forwarding packet sedangkan router LER bertanggung jawab dalam menambah atau menghapus label pada packet yang memasuki atau meninggalkan domain MPLS. Masing-masing router dikonfigurasi protokol routing OSPF, selanjutnya dilakukan percakapan melalui aplikasi IP Telephony pada komputer user. Pada saat proses percakapan terjadi diamati paket RTP untuk menghitung Quality of Service (QoS) yang meliputi, throughput, delay, paket loss dan jitter. Setelah itu pada masing-masing router dikonfigurasi MPLS dan paket RTP diamati kembali. Hasil eksperimen pada bagian pertama ditunjukkan pada TABEL 1.

TABEL 1. HASIL IMPLEMENTASI PROTOKOL OSPF

| Parameter | no mpls | | with mpls | |
|-------------------|---------|--------|-----------|--------|
| | user 1 | user 2 | user 1 | user 2 |
| Throughput (kbps) | 76,8 | 86 | 92,32 | 86,51 |
| Packet Loss (%) | 0 | 0 | 0 | 0 |
| Delay (s) | 0,02 | 0,02 | 0,02 | 0,02 |
| Jitter (ms) | 18,40 | 20,73 | 9,67 | 11,38 |

Pada eksperimen berikutnya, jaringan VOIP MPLS menggunakan protokol routing BGP. Router yang digunakan sebanyak 7 buah, yang terdiri dari 3 buah router LSR yang berfungsi untuk meneruskan paket, 2 buah router LER yang berfungsi untuk menambahkan atau menghapus label dan 2 buah router CE yang terhubung langsung dengan klien. Hasil eksperimen jaringan VOIP MPLS VPN menggunakan protokol BGP ditunjukkan pada Tabel 3.

TABEL 1. HASIL EKSPERIMEN MENGGUNAKAN PROTOKOL BGP

| Parameter | mpls | | mpls vpn | |
|-------------------|-----------|-----------|------------|-----------|
| | user 1 | user 2 | user 1 | user 2 |
| throughput (Kbps) | 77 | 88 | 64 | 56 |
| packet loss (%) | 0 | 0 | 0 | 0 |
| delay (s) | 0,02 s | 0,02 s | 0,0 2 s | 0,0 2 |
| jitter (ms) | 19,8 2 | 16,9 8 | 7,1 3 | 13, 09 |

Penerapan MPLS VPN pada jaringan VOIP menggunakan protokol BGP mempengaruhi nilai throughput dan jitter. Sedangkan delay dan packet loss cenderung sama baik saat menerapkan L2TP/IPSec maupun tanpa menggunakan L2TP/IPSec. Nilai throughput mengalami penurunan sebesar 27% sedangkan nilai jitter mengalami perbaikan sebesar 45%. Penurunan nilai throughput ini disebabkan karena membutuhkan bandwidth yang lebih besar saat melakukan tunneling menggunakan L2TP/IPSec. Namun demikian, saluran komunikasi lebih aman karena paket-paket data VOIP dikirimkan melalui tunnel dan dienkripsi.

Eksperimen selanjutnya dengan menerapkan L2TP/IPSec pada jaringan VOIP MPLS. L2TP/IPSec bertanggung jawab dalam melakukan enkripsi dan tunneling pada jaringan VOIP MPLS. L2TP/IPSec server berjalan pada Router PE. Sedangkan L2TP/IPSec client berjalan pada sisi user. Open VPN bertanggungjawab dalam mengamankan saluran komunikasi VOIP MPLS. Hasil eksperimen penerapan L2TP/IPSec pada jaringan VOIP MPLS ditunjukkan pada TABEL 2.

TABEL 2. PERBANDINGAN QOS MPLS DAN MPLS VPN

| Parameter | mpls | | mpls vpn | |
|-------------------|-----------|-----------|----------|--------|
| | user 1 | user 2 | user 1 | user 2 |
| throughput (Kbps) | 92,32 | 86,51 | 6,144 | 6,784 |
| packet loss (%) | 0 | 0 | - | - |
| delay (s) | 0,02 s | 0,02 s | - | - |
| jitter (ms) | 9,67 | 11,38 | - | - |

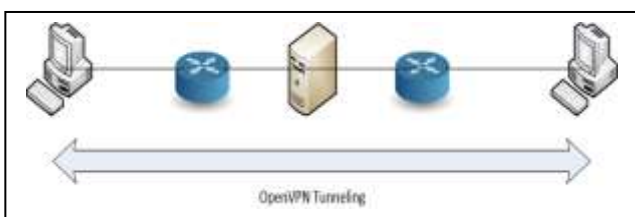
B. Pembahasan

Penambahan label pada header paket mampu memperbaiki nilai throughput dan jitter pada protokol routing OSPF baik pada penerapan L2TP/IPSec maupun tanpa penerapan L2TP/IPSec. TABEL 1 menunjukkan bahwa penerapan MPLS pada jaringan VOIP mampu meningkatkan nilai throughput dan memperbaiki nilai jitter. Sedangkan untuk parameter packet loss dan delay cenderung sama. Hal ini dikarenakan kesederhanaan jaringan yang dibuat serta jumlah user yang kecil, 2 user. Peningkatan nilai throughput dan jitter ini dikarenakan saat packet memasuki domain MPLS, router LER atau PE akan menambahkan label pada header packet yang memudahkan router LSR atau P dalam melakukan packet forwarding. Di sisi lain, router LER atau PE akan menghapus label pada packet yang meninggalkan domain MPLS. Berdasarkan TABEL 1, penerapan MPLS pada jaringan VOIP

meningkatkan nilai throughput sebesar 10% dan perbaikan nilai jitter sebesar 40%.

Selanjutnya pada jaringan VOIP MPLS diterapkan tunneling menggunakan L2TP/IPSec. Tunneling L2TP/IPSec ini digunakan untuk menghubungkan langsung secara virtual antara user dengan server. Berdasarkan hasil eksperimen diperoleh bahwa dengan penerapan Open VPN pada jaringan VOIP MPLS mampu meningkatkan nilai throughput dan jitter. Peningkatan nilai throughput sebesar 3% dan perbaikan jitter sebesar 26%. Sementara nilai parameter packet loss dan delay cenderung sama, hal ini dikarenakan kesederhanaan jaringan serta kecilnya jumlah user. L2TP/IPSec membuat tunnel serta melakukan enkripsi pada packet VOIP sehingga packet data tidak dapat disadap oleh pihak ketiga. Meskipun L2TP/IPSec melakukan enkripsi, dimana membutuhkan proses yang lebih lama ternyata nilai throughput tidak lebih kecil bahkan lebih besar dibandingkan tanpa melakukan enkripsi. Hal ini dikarenakan selain melakukan enkripsi, L2TP/IPSec juga membuat tunnel yang menghubungkan secara langsung antara user dengan server secara virtual. Selain itu L2TP/IPSec menggunakan protokol UDP yang bersifat connectionless sehingga pengiriman data yang dilakukan bisa lebih cepat meskipun tidak ada pemeriksaan kesalahan pengiriman. Tunneling menggunakan UDP lebih efisien dan mampu meningkatkan waktu transfer serta kecepatan transfer dibandingkan menggunakan TCP[11].

Dalam melakukan tunneling L2TP/IPSec membuat virtual address yang berbeda dengan IP address. Pada penelitian ini IP Address yang digunakan 192.168.0.2 pada user 1 dan 192.168.0.2 pada user 2. Sedangkan virtual address yang dibuat 10.8.0.6 pada user 1 dan 10.8.0.10 pada user 2. Virtual address digunakan untuk mengirimkan packet melalui tunnel. Model tunneling L2TP/IPSec ditunjukkan pada gambar 2.



Gambar 2. Model tunneling L2TP/IPSec

Packet-packet VOIP dikirimkan melalui tunneling sehingga lebih aman dari penyadapan. Penerapan L2TP/IPSec dalam melakukan pengiriman packet melalui tunnel ditunjukkan pada Gambar 3. Koneksi tunneling menggunakan UDP pada port 1194. Koneksi ini tidak bisa disadap karena bersifat connectionless berbeda dengan koneksi tunneling TCP yang bersifat connection oriented. Connectionless artinya dalam pengiriman packet tidak diperlukan adanya koneksi terlebih dahulu, sehingga akan

menghemat waktu transfer serta mempercepat kecepatan transfer.

Berdasarkan karakteristik Tunneling L2TP/IPSec menggunakan UDP yang bersifat connectionless maka nilai throughput dan nilai jitter menjadi lebih baik saat menerapkan L2TP/IPSec pada jaringan VOIP MPLS.

V. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan dapat disimpulkan bahwa secara keseluruhan penerapan MPLS VPN mampu meningkatkan Quality of Service (QoS) protokol routing OSPF pada jaringan VoIP, khususnya pada parameter throughput dan jitter. Peningkatan nilai throughput sebesar 3% dan perbaikan jitter sebesar 26%. Selanjutnya perlu dilakukan traffic engineering pada jaringan VOIP MPLS VPN.

UCAPAN TERIMA KASIH

Terima kasih kami sampaikan kepada Pusat Penelitian dan Pengabdian Masyarakat yang telah mendanai penelitian ini melalui skema PNBPN tahun 2017.

DAFTAR PUSTAKA

- [1] R. Yunos, S. A. Ahmad, N. M. Noor, R. M. Saidi dan Z. Zainol, "Analysis of Routing Protocol of VOIP VPN over MPLS Network," dalam *2013 IEEE Conference on Systems, Process & Control (ICSPC)*, Kuala Lumpur, 2013.
- [2] M. M. Al-Quzwini and S. A. Sharafali, "Performance Evaluation of MPLS TE Signal Protocols with Different Audio Codecs," *Journal of Emerging Trends in Computing and Information Sciences Vol. 5 No. 6*, pp. 447-463, 2014.
- [3] G. Liu and X. Lin, "MPLS Performance Evaluation in Backbone Network," in *ICC 2002. IEEE International Conference on Communications, 2002.*, New York, 2002.
- [4] G. Armitage, "MPLS: The Magic Behind the Myths," *IEEE Communications Magazine*, Vols. Volume: 38., no. Issue: 1, pp. 124-131, Januari 2000.
- [5] M. K. Porwal, A. Yadav and S. Charhate, "Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS," in *First International Conference on Emerging Trends in Engineering and Technology*, Nagpur, Maharashtra, India, 2008.
- [6] A. M. Sillame, "Modeling and Simulating MPLS Networks," in *The 2014 International Symposium on Networks, Computers and Communications*, Hammamet, Tunisia, 2014.
- [7] M. Kim, D. Kim and G. E. Sobelman, "Network-on-chip quality-of-service through multiprotocol label switching," in *2006 IEEE International Symposium on Circuits and Systems*, Island of Kos, Greece, 2006.
- [8] R. Mishra and H. Ahmad, "Comparative Analysis of Conventional IP Network and MPLS Network over VoIP Application," (*IJCSIT International Journal of Computer Science and Information Technologies*, vol. Vol 5, no. No 3, pp. 4496-4499, 2014.

-
- [9] J. Aggarwal and A. Dhall, "Performance Analysis of MPLS over VOIP," *International Journal of Science, Engineering and Technology Research (IJSETR)* Vol. 4 (6), pp. 1896-1901, 2015.
- [10] S. Ahmad, W. A. Hamdani and M. H. Magray, "Performance Evaluation of IPv4 and IPv6 over MPLS using OPNET," *International Journal of Computer Applications* Vol. 125 No. 3, pp. 34-38, 2015.
- [11] I. Coonjah, P. C. Catherine and K. S. Soyjaudah, "Experimental performance comparison between TCP vs UDP tunnel using L2TP/IPSec," in *2015 International Conference on Computing, Communication and Security (ICCCS)*, Pamplemousses, Mauritius, 2015.