IMPLEMENTASI DAN ANALISA PERFORMANSI LAYANAN VPN PADA JARINGAN MPLS-TE MENGGUNAKAN PROTOKOL BGP DENGAN METODE QOS INTSERV

ANALISYS AND IMPLEMENTATION VPN SERVICE PERFORMANCE OF MPLS-TE NETWORK USING BGP PROTOCOL BY INTSERV QOS METHODE

Salsa Rizkiana[1],Doan Perdana[2], Ridha Negara.[3]

[1,2,3] Fakultas Teknik Elektro, Telkom University Bandung
[1]rizkianaasalsa@gmail.com, [2]doanperdana@telkomuniversity.ac.id,
[3]ridhanegara@telkomuniversity.ac.id

Abstrak

Fitur Traffic Engineering pada MPLS dapat melakukan perpindahan pada link trafik yang mengalami *congestion*, sehingga link dapat dipindahkan pada link yang kosong. Teknologi MPLS VPN-TE menjadisolusi untuk meningkatkan keamanan dan pemilihan rute terbaik dalam suatu jaringan. *Integrated Service* merupakan salah satu model QoS untuk masalah pengontrolan bandwidth end-to-end pada suatu jaringan yang diperlukan oleh teknologi MPLS VPN-TE untuk kestabilan jaringan. Open IMS Core merupakan server layanan multimedia yang digunakan pada teknologi MPLS VPN-TE dengan mempertimbangkan *Quality Of Service* pada layanan multimedia. Penggunaan protocol BGP merupakan jenis peroutinganyang dapat melakukan pertukaran informasi routing dengan memetakan tabel IP network antar *Autonomous System* (AS) dengan memberikan peningkatan QoS pada suatu jaringan.Pada Penelitian inidiimplementasikan teknologi MPLS VPN TE dengan menggunakan router mikrotik. Dari hasil pengujian menunjukan bahwa teknologi MPLS VPN dengan penambahan fitur Traffic Engineering didapatkan hasil perbaikan delay sebesar 27,44% untuk voip,11,14% untuk video call. Untuk parameter throughput mengalami perbaikan sebesar 6,02 % untuk voip, 56,6% untuk video call dan jitter mendapatkan hasil < 1 ms.Dengan menggunakan router mikrotik dan server OpenIMS core penerapan Routing protocol BGP pada Jaringan MPLS VPN melalui teknologi Traffic Engineering metode QoS Intserv dapat diimplementasikan layanan VoIP dan Video call. Parameter Jitter untuk layanan VoIP dan Video Call telah memenuhi standar ITU-T G.1010 yaitu dibawah 1 ms.

Kata Kunci :MPLS VPN, MPLS VPN-TE, Integrated Service, QoS, Open IMS Core, BGP

Abstract

The Traffic Engineering feature on MPLS can move a traffic link that has congestion avoidance, therefore a link can be moved to an empty link. The MPLS VPN TE technology is the solution in increasing security and choosing the best route in a network. Integrated service is one of a QoS model for bandwidth controlling problem on a network that is needed for MPLS VPN-TE technology for stability of network. Open IMS Core is a multimedia service server that is used on MPLS VPN TE technology by considering Quality Of Service on multimedia. The usage of BGP protocol is a type of routing that is expected to do an exchange of routing information by mapping an IP table network inter-Autonomous System by giving Qos enhancement on a network In this research, the author implements MPLS VPN TE on Mikrotik Router. The test result of Traffic Engineering feature on MPLS VPN network show improved 27,44 % in delay for Voip services, 11,14% for video call services. For Throughput parameter showed a improved 6,02% for Voip

service, 56,6 for video call services. For jitter parameters result < 1ms. With using mikrotik router and OpenIMS core server can be implemented BGP routing protocol on VPN MPLS network. Through using QoS Intserv method as part of traffic engineering can results VoIP and Video Call services. Jitter parameter for VoIP and video call services has fullfil ITU-T G.1010 standard in under 1 ms.

Key words :MPLS VPN, MPLS VPN-TE, Integrated Service, QoS, Open IMS Core, BGP

1. PENDAHULUAN

Perkembangan teknologi telekomunikasi dan informasi untuk melakukan kelancaran proses kerja, maka dibutuhkan dukungan komunikasi dan proses transfer data secara real time maupun fungsi keamanan yang terjamin. Maka dibutuhkan jaringan pribadi yang menghubungkan antar user ataupun instansi. Hal ini membutuhkan investasi yang mahal dalam jaringan, sehingga *user* membutuhkan jaringan publik yang bersifat pribadi untuk mengatasi hal tersebut. Teknologi MPLS (*Multi ProtocolLabel Switching*) merupakan metode untuk meneruskan data melalui suatu jaringan dengan menggunakaninformasi dalam label yang dilekatkan pada IP. Teknologi ini membutuhkan konsep VPN (*Virtual PrivateNetwork*) untuk transfer data yang tinggi serta memungkinkan user menggunakan jaringan publik yangbersifat pribadi dengan network private IP yang sama tanpa adanya link terpisah dan keamanan kualitas data yang terjamin, serta membatasi pemborosan link yang tidak dipakai bagi setiap user pada jaringan yang sama [1] . Performansi kualitas dari suatu jaringan juga merupakan salah satu hal yang perlu diperhatikan.

MPLS menyediakan fitur *Traffic Engineering* yang menjadi solusi untuk menyeimbangkan beban trafik agar sesuai dengan kebutuhan jaringan dan menyediakan efisiensi dalam penggunaan perfomansi trafik. Dengan kata lain, trafik yang memiliki congestion akan dipindahkan ke link yang sedang tidak digunakan sehingga dapat memanfaatkannya link yang berlebih [2]. Disamping itu MPLS juga membutuhkan jaminan bandwidth untuk paket-paket yang dikirimkan maka digunakannya Metode QoS Intserv secara *end-to-end* untuk memudahkan pengontrolan bandwidth pada MPLS. BGP merupakan protocol routing yang beroperasi pada *Autonomous Systems* (AS) yang memiliki skabilitas dan integritas yang tinggi sehingga dapat melayani pertukaran routing pada teknologi MPLS untuk mekanisme autentikasi dalam menjaga integritas suatu jaringan[3]. Terdapat beberapa mekanisme untuk kondisi jaringan yang stabil, yaitu mengatur teknologi *Traffic Engineering* dengan pemilihan rute terbaik dalam sebuah jaringan MPLS yang dilewati layanan VPN dengan routing protocol BGP dan menjaga nilai QoS dengan metode *Intserv*. Berdasarkan problema di lapangan baik untuk kebutuhan instansi maupun jaringan pribadi yang semakin pesat perkembangannya dan sangat sering menimbulkan *congesti*, maka untuk mengatasi hal itu metode Intserv QoS dengan menggunakan protocol BGP dipilih untuk dapat memberikan solusinya dengan melalui implementasi skala laboratorium menggunakan mikrotik router dan openIMS core server.

2. LANDASAN TEORI

2.1 Multi Protocol Label Switching (MPLS)

Multi Protocol Label Switching (MPLS) adalah suatu metode forwarding (meneruskan data melalui suatu jaringandengan menggunakan informasi dalam label yang dilekatkan pada paket IP[2][4]. Label pada paket IP ini memungkinkan router untuk meneruskan traffic dengan melihat label dari paket itu sendiri,tidak perlu melihat IP alamat tujuan. MPLS menggabungkan teknologi switching di layer 2 dan teknologi routing di layer 3 sehingga menjadi solusi jaringan terbaik dalam menyelesaikan masalah kecepatan, scability, Quality Of Service (QoS) dan rekayasa trafik.

2.2 Virtual Private Network (VPN)

Virtual Private Network adalah jaringan dimana sebagai tempat konektivitas customer yang dapat berhubungan satu sama lain dalam suatu share infrastruktur dengan security dan kebijakan yang sama dengan private network. VPN menyediakan komunikasi di OSI Layer 2 atau 3. Menurut Internet Engineering Task Force (IETF), VPN merupakan suatu bentuk private internet yang melalui jaringan public (internet), dimana customer mampu melakukan interkoneksi dengan vpn lain dengan menekankan pada keamanan data dan akses global melalui internet [5].

2.3 MPLS-VPN

MPLS-VPN adalah sebuah teknologi Multiprotocol Label Switching (MPLS) untuk membuat jaringan pribadi virtual (VPN) yang menghasilkan costumer routing yang lebih sederhana, provisioning yang lebih sederhana oleh service provider, dan memungkinkan sejumlah topologi yang sulit diimplementasikan dalam bentuk VPN peer to peer [6]. MPLS beroperasi secara connectionless sedangkan pada VPN beroperasi secara connection oriented.

2.4 MPLS-TE

Routing di jaringan IP diatur oleh kebutuhan untuk mendapatkan trafik di seluruh jaringan dengan cepat. SetiapIP routing protokol memiliki cost yang terkait dengan link dalam jaringan [1]. Traffic Engineering adalah solusi untuk permasalahan diatas dengan MPLS yaitu trafik dari link yang memiliki congestion dipindahkan ke link yang tidak digunakan untuk menghemat cost. MPLS mengkombinasikan kemampuan traffic engineering dengan fleksibilitas IP dan pembagian kelas layanan [7].

MPLS-TE memungkinkan Traffic Engineering dimana the head end router pada LSP dapat menghitung rute yangpaling efisien ke router akhir LSP. The head end router perlu mengetahui bandwidth yang tersisa pada link. Sehingga the head end router dapat menentukan LSP yang digunakan. Kemudian MPLS dapat membangun LSP dari ujung ke ujung[8].

2.5 Integrated Service

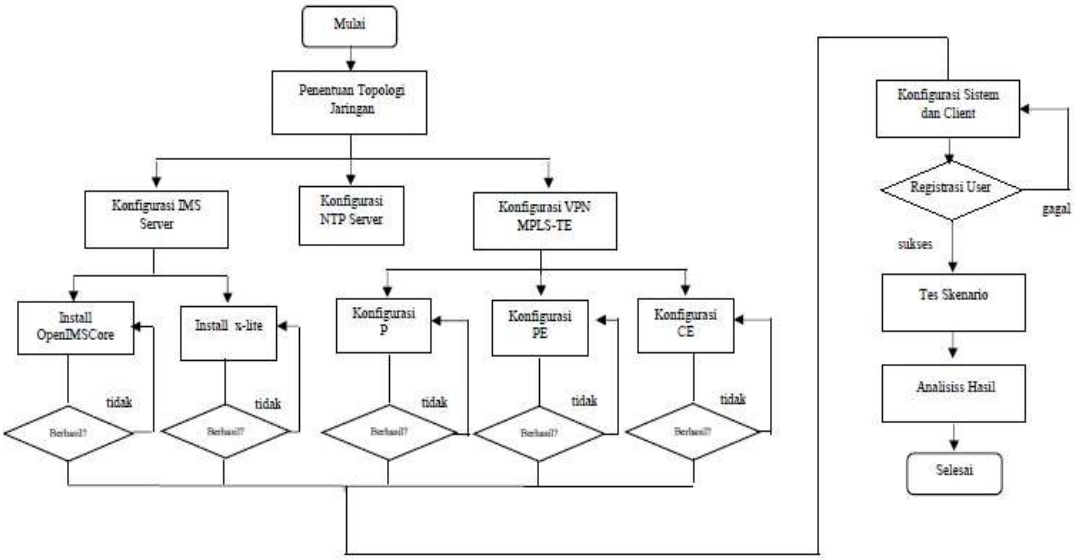
Integrated Service merupakan metode untuk mengelola QoS pada network IP yang bertujuan untuk menyediakan kebutuhan sumber daya seperti bandwidth untuk traffic end-to-end pada user. Intserv harus mengirimkan proses signaling pada jaringan sebelum melakukan pengiriman paket data. Resource Reservation Protocol (RSVP) bertanggungjawab dalam proses signaling tersebut karena RSVP bertugas memberi tahu kepada setiap router yang dilewati mengenai kebutuhan bandwidth setiap aplikasi. Pada layanan ini bandwidth akan dipesan untuk menjamin paket-paket yang dikirimkan[9].

2.6. Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) merupakan sebuah protocol routing yang digunakan untuk mentransfer data informasi antara gateway dengan host yang berbeda dan lalu lintas rute di internet atau Autonomous System (AS)[10].

3. PERANCANGAN DAN IMPLEMENTASI

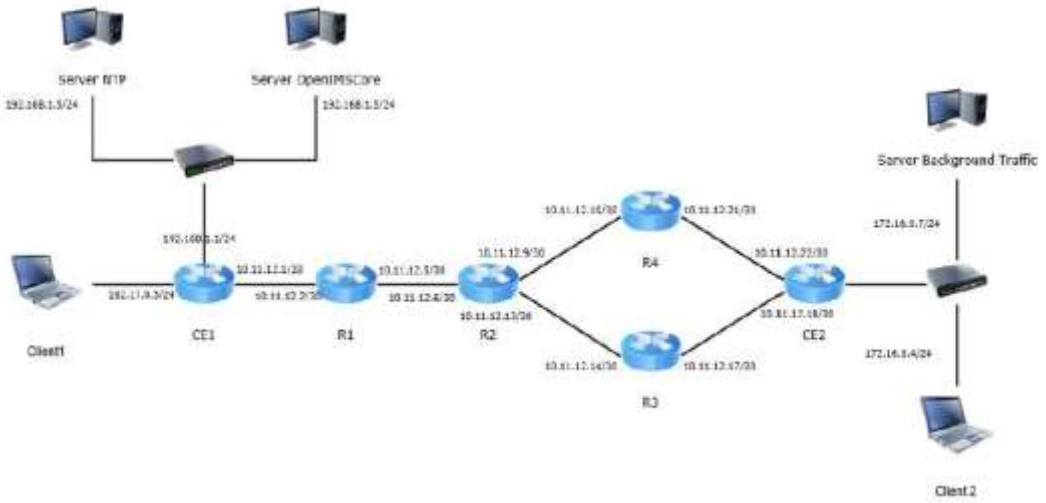
Perancangan sistem dituangkan melalui gambar flowchart dibawah ini:



Gambar 1. Flowchart Perancangan Sistem

Berdasarkan Flow chart yang telah dibuat, maka dapat dijelaskan secara ringkas sebagai berikut :
a. Penentuan topologi jaringan dan komponennya
b. Konfigurasi jaringan VPN MPLS beserta perangkat lunak penunjangnya.
c. Install Open IMS core dan konfigurasi semua router dalam jaringan VPN MPLS.
d. Lakukan testing terhadap perangkat lunak dan komponen jaringan
e. Konfigurasi Sistem dan Client serta registrasi user
f. Lakukan scenario pengujian dan analisa hasil
g. Selesai

3.1 Topologi Perancangan



Gambar 2. Topologi Perancangan Jaringan

Topologi diatas menjelaskan bahwa jaringan MPLS VPN TE menghubungkan antar client dengan server OpenIMSCore pada IP 192.168.1.5/24. Dimana Backbone MPLS VPN ini menggunakan 6 buah router mikrotik dengan konsep MPLS VPN dengan penamaan CE1 dan CE2

bertindak sebagai Customer Edge, Router R1,R4 dan R3 bertindak sebagai Provider Edge dan R2 bertindak sebagai Provider yang bertugas untuk menjadi Route-Reflect agar dapat melakukan "Peering" dengan setiap router yang ada.

Tabel 1. Tabel pengalamatan MPLS VPN TE Backbone

Router	Interface			
	Ether 1	Ether 2	Ether 3	Loopback
CE1	192.168.1.1/24	10.11.12.1/30	182.17.0.1/24	10.10.10.5
R1	10.11.12.2/30	10.11.12.5/30		10.10.10.1
R2	10.11.12.6/30	10.11.12.9/30	10.11.12.13/30	10.10.10.2
R3	10.11.12.14/30	10.11.12.17/30		10.10.10.3
R4	10.11.12.10/30	10.11.12.21/30		10.10.10.4
CE2	10.11.12.22/30	10.11.12.18/30	172.16.0.1/24	10.10.10.6

Tabel 2. Tabel Pengalamatan Device

Device	Ip Address
Server Open IMSCore	192.168.1.5
Server NTP	192.168.1.5
Server Background Traffic	172.16.0.7
Client 1	182.17.0.5
Client 2	172.16.0.4

3.2 Skenario Pengujian

Pengujian dilakukan dengan dua skenario yaitu :

a. Pengujian jaringan MPLS VPN Tanpa Traffic Engineering

b. Pengujian jaringan MPLS VPN dengan Traffic Engineering

Pada setiap skenario pengujian, akan dilakukan skenario tanpa pembanjiran traffic (0 Mbps) dan dengan pembanjiran trafik menggunakan iperf sebesar 20 Mbps,40 Mbps,60 Mbps,80 Mbps, dan 95 Mbps. Pengujian dilakukan sebanyak 30 kali dengan interval 1 menit untuk setiap kali pengambilan data pada setiap skenario pembanjiran trafik yang berbeda.

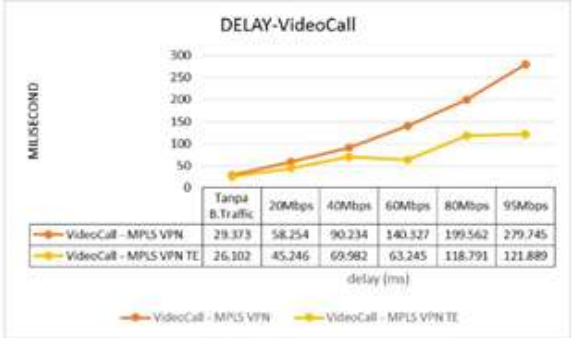
4. PENGUJIAN DAN ANALISIS

Pada bab ini akan dibahas analisis jaringan menggunakan backbone MPLS Virtual Private Network dengan tambahan teknologi traffic engineering. Analisis yang dilakukan bertujuan untuk mengetahui performansi layanan multimedia yang terdiri atas Voice Over IP dan Video Call. Analisis tersebut berdasarkan beberapa parameter QoS yaitu One way delay, Jitter, Throughput dan perhitungan MOS yang bertujuan untuk menentukan kualitas dari layanan.

4.1 Delay

Berikut ini merupakan hasil pengukuran parameter QoS yaitu delay dengan skenario pengujian yang telah dijelaskan.

Gambar 3 Grafik Delay VoIP

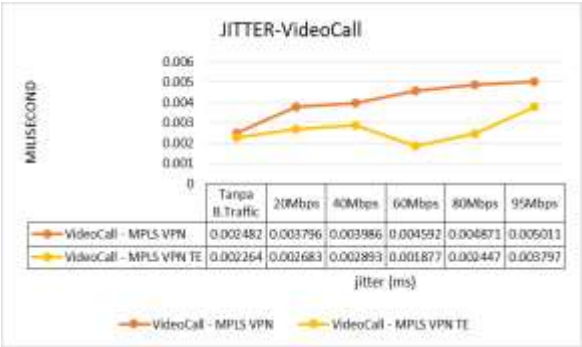


Gambar 4 Grafik Delay Videocall

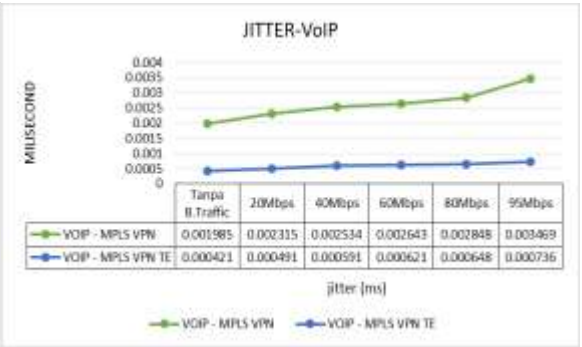
Dari gamber.3 dapat diketahui bahwa nilai delay layanan VoIP jaringan MPLS VPN-TE mengalami perbaikan nilai sebesari 27,44% dibandingkan nilai delay pada jaringan MPLS VPN tanpa TE. Sedangkan pada gambar.4 untuk nilai delay layanan video call pada jaringan MPLS VPN-TE mengalami perbaikan sebesar 11,14% dibandingkan nilai delay jaringan tanpa TE. Hal ini disebabkan karena Traffic Engineering menggunakan mekanisme pemilihan state terbaik maka dilakukan manipulasi trafik sehingga sebagian trafik dilewatkan kepada link-link yang memiliki utilitas jaringan yang paling rendah, sehingga menghasilkan waktu tempuh paket sampai ke tujuan lebih cepat. Maka nilai delay relatif lebih kecil dibandingkan MPLS VPN tanpa TE.

4.2 Jitter

Berikut ini merupakan hasil pengukuran parameter QoS yaitu jitter dengan skenario pengujian yang telah dijelaskan diatas.



Gambar 5 Grafik Jitter VoIP

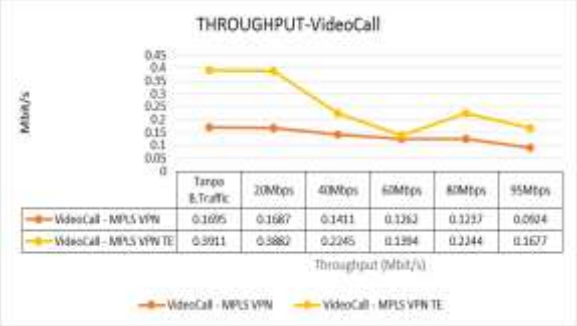


Gambar 6 Grafik Jitter Videocall

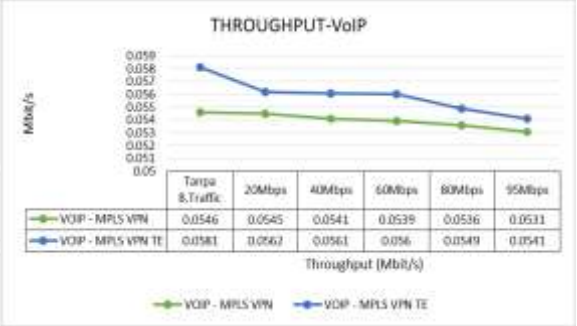
Jitter merupakan variasi delay yang terjadi akibat adanya selisih waktu atau interval antar kedatangan paket di tujuan. Sehingga, nilai jitter dapat dipengaruhi oleh nilai delay pula. Dari gambar.5 dapat diketahui bahwa nilai jitter relatif naik seiring besarnya background traffic yang ditambahkan pada jaringan. Terlihat pada skenario layanan VoIP, nilai jitter pada jaringan MPLS VPN-TE lebih kecil dibandingkan dengan nilai jitter pada MPLS VPN tanpa Traffic Engineering. Sedangkan pada gambar.6 terlihat bahwa layanan Video Call, nilai jitter di jaringan MPLS VPN-TE mengalami fluktuasi namun cenderung meningkat pada background traffic 60 Mbps dan 80 Mbps. Hal ini disebabkan besarnya nilai jitter sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congetion) yang ada pada jaringan IP akibat antrian paket yang dikirim pada aliran paket data.

4.3 Throughput

Berikut ini merupakan hasil pengukuran parameter QoS yaitu jitter dengan skenario pengujian yang telah dijelaskan di atas.



Gambar 7. Grafik Throughput VoIP



Gambar 8. Grafik Throughput Videocall

Throughput lebih menggambarkan bandwidth yang sebenarnya (aktual) pada suatu waktu tertentu dan pada kondisi jaringan tertentu. Dari gambar.7 dapat terlihat dari grafik bahwa nilai throughput untuk layanan VoIP yang dilewatkan pada jaringan MPLS VPN TE dan tanpa TE memiliki hasil yang relatif sama yaitu sekitar 0.05 Mbit/s dan mengalami perbaikan sebesar 6,13% pada jaringan MPLS VPN TE. Berbeda halnya dengan gambar.8 bahwa nilai throughput pada jaringan MPLS VPN-TE yang dilewatkan layanan Video mengalami perbaikan sebesar 56,6%. Hal ini disebabkan karena MPLS VPN TE dapat mengatur link state yang akan dilewatkan oleh paket. Selain itu penggunaan Metode QoS Intserv mempengaruhi pengaturan bandwidth yang di lewati, Metode QoS Intserv bersifat end-to-end dari pengirim hingga ke penerima sehingga bandwidth yang dilewati sudah di reservasi terlebih dahulu sebelum mengirimkan paket.Namun nilai throughput dengan skenario 80 Mbps pada layanan MPLS VPN TE mengalami fluktuasi anomali data, hal ini disebabkan karena sebuah perangkat tidak dikalibarasi sebelum melakukan pengambilan data. Selain itu, LAN menyediakan transfer data 100 Mbps, namun pada kenyataannya hanya dapat melakukan transfer data rata-rata 80 Mbps-90 Mbps. Sehingga bisa dikatakan jaringan MPLS VPN-TE memiliki kualitas jaringan yang lebih baik dibandingkan MPLS VPN tanpa Traffic Engineering.

4.4 Mean Opinion Score

Dalam jaringan IP, dibutuhkan Mean Opinion Score untuk mengetahui kualitas layanan. Pendekatan matematis yang digunakan untuk menentukan kualitas suara berdasarkan penyebab menurunnya kualitas suara dalam jaringan VoIP dimodelkan dengan E-Model yang berstandar kepada ITU-T G.107. Nilai akhir estimasi E-Model disebut dengan R factor.

Secara umum, nilai estimasi R factor menjadi[11] :

$$R = 94{,}2 - [0{,}024\,d + 0{,}11\,(d-177{,}3)\,H\,(d-177{,}3)] - [7+30\ln(1+15e)] \quad (1)$$

Dengan :

R = factor kualitas transmisi
d = delay (millisecond)
H = fungsi tangga ; dengan ketentuan
H(x) = 0 jika x < 0,lainnya

H(x) = 1 untuk x > 0
e = persentasi besarnya paket loss yang terjadi (dalam bentuk decimal)

Tabel 3. Hasil Perhitungan MOS

Voip									
	Delay	d-177.3	H(x)	Id	Packet Loss	30 ln(1+15e)	Ief	R Faktor	MOS
MPLS VPN	27.066	-150.234	0	0.649584	0	0	7	86.550416	4.054261
MPLS VPN-TE	19.637	-157.663	0	0.471288	0	0	7	86.728712	4.0603356
Video Call									
MPLS VPN	29.373	-147.927	0	0.704952	0	0	7	86.495048	4.0523737
MPLS VPN-TE	26.102	-151.198	0	0.626448	0	0	7	86.573552	4.0550495

5. KESIMPULAN

Dari hasil perancangan dan implementasi melalui pengukuran parameter performansi, maka dapat disimpulakan sebagai berikut :

1. Dengan menggunakan router mikrotik dan server OpenIMSCore penerapan Routing protocol BGP pada Jaringan MPLS VPN melalui teknologi Traffic Engineering metode QoS Intserv dapat diimplementasikan layanan VoIP dan Video call.
2. Penggunaan teknologi Traffic Engineering dan metode QoS Intserv pada jaringan MPLS VPN terbukti dapat membuat perbaikan performansi layanan VoIP dan Video call yaitu dengan berbagai skenario penambahan background traffic. Pada pada skenario 0Mbps (tanpa background traffic) nilai delay memberikan perbaikan sebesar 7,42 ms atau 27,44 % untuk layanan voip dan untuk layanan video call sebesar 3,2737 atau 11,14%.
3. Dari segi parameter throughput pada skenario 0 Mbps (tanpa backgroundtraffic) dengan teknologi Traffic Engineering pada jaringan MPLS VPN memberikan perbaikan sebesar 0.003 Mbit/s atau 6,02% untuk layanan VoIP dan layanan Video Call sebesar 0,221 Mbit/s atau 56,6 %.
4. Parameter Jitter untuk layanan VoIP dan Video Call telah memenuhi standar ITU-T G.1010 yaitu dibawah 1 ms.
5. Penambahan skenario background traffic 20-80 Mbps menghasilkan nilai delay dan jitter yang semakin besar atau berbanding lurus dengan background traffic sedangkan untuk nilai throughput menghasilkan nilai yang semakin kecil. Hal ini disebabkan oleh utilitas jaringan yang tinggi, sehingga menyebabkan antrian node menjadi bertambah yang pada akhirnya dapat mempengaruhi penyempitan bandwidth pada saluran transmisi, sehingga mengakibatkan traffic pengiriman data akan padat.

DAFTAR PUSTAKA

[1] S. Yadav and A. Jeyakumar, “Design of Traffic Engineered MPLS VPN for Protected Traffic using GNS Simulator,” Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference. pp. 405–409, 2016.

[2] R. Munadi, Teknik Switching. Bandung:Buku Cetak, Penerbit Informatika Bandung, 2011.

[3] S. Maheshwarn, S. Lillypet, and C. Vennila, “QOS Capabilities for Building MPLS VPN,” International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391 vol. 5, no. 5, pp. 2247–2251, 2016.

[4] A. Madsen, T. AB Acreo, "Provider Provisioned Virtual Private Network (VPN) Terminologi, Network Working Group," 2005. [Online]. Available: https://tools.ietf.org/html/rfc4026.
[5] Cisco Corporation (2002). "MPLS-VPN Technology". Cisco System.
[6] J. T. Elektro, F. Teknik, and U. S. Kuala, "Pengujian Performansi Jaringan Testbed MPLS-VPN Pada Laboratorium Jaringan Komputer," no. Snastikom, pp. 1–6, 2012.
[7] C. System, Advanced Topics in MPLS-TE Deplomen. USA, 2009.
[8] C. Press, MPLS Fundamental A Comprehensive Introduction to MPLS Theory and Practice. USA,2006.
[9] C.System,"qos_rsvp."[Online].Available: http://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/convert/qos_rsvp/config_rsvp. html. [Accessed: 01-Oct-2016].
[10] Cisco. (2001). Document ID: 26634. Retrieved from BGP Case Studies: http://www.cisco.com/e/en/us/support/docs/ip/border-gateway-protocolbgp/26634-bgp-toc.html
[11] ITU-T, "The E-model, a computational model for use in transmission planning," in SERIES G :TRANSMISSION SYSTEM AND MEDIA, DIGITAL SYSTEMS AND NETWORKS, 2009, pp. pp 1-11