Analisis *Quality of Service (QoS)* pada Jaringan *VPN* dan *MPLS VPN* Menggunakan GNS3

Mardianto

Universitas Sembilanbelas November Kolaka, Fakultas Teknologi Informasi
Jl. Pemuda No 339, Kolaka
mardianto.itsc@gmail.com

Abstrak

Internet yang terus menerus meningkat merupakan tantangan *Internet Service Provider (ISP)* untuk masa depan akan kebutuhan lalu lintas jaringan komputer global dan *Quality of Service* (*QoS)* yang diharapkan. Untuk menjaga agar kompetitif *ISP* di indonesia dengan perkembangan pemakaian internet menyebabkan permintaan *QoS* harus ditingkatkan. Jaringan *MPLS VPN* menggabungkan teknologi *switching* layer 2 dengan teknologi *routing* layer 3. Jaringan *MPLS VPN* muncul sebagai teknologi yang memenuhi persyaratan *VPN* seperti *private IP*, dan kemampuan untuk mendukung alamat yang bertumpuk dalam menyelesaikan masalah kecepatan dan *QoS*. Metode yang digunakan adalah riset ekperimental. Dari hasil pengukuran diperoleh *delay* jaringan *VPN* dan *MPLS VPN* memilik nilai *delay* sangat bagus. Untuk *throughput* pada jaringan *VPN* memiliki kualitas sedang dan pada jaringan *MPLS VPN* memiliki kualitas Bagus. Dan untuk nilai *packet loss* untuk kedua jenis jaringan adalah 0 %. Hal ini menunjukan bahwa *throughput* jaringan *MPLS VPN* memiliki *QoS* yang lebih Bagus sedangkan untuk *delay* dan *packet loss* pada jaringan *VPN* dan *MPLS VPN* memiliki nilai kualitas yang sama.

Kata kunci: *VPN, MPLS VPN, delay, throughput, packet loss*

Abstract

The ever-increasing internet is an ISP challenge for the future of the expected global computer network traffic and QoS needs. To maintain competitive ISPs in Indonesia with the development of internet usage, the demand for QoS must be increased. MPLS VPN networks combine layer 2 switching technology with layer 3 routing technology. MPLS VPN networks have emerged as technologies that meet VPN requirements such as private IP, and the ability to support overlapping addresses in resolving speed and QoS problems. The method used is experimental research. From the measurement results obtained by VPN and MPLS VPN network delay has a very good delay value. For throughput on VPN networks have medium quality and MPLS VPN networks have good quality. And for the packet loss value for both types of networks is 0%. This shows that MPLS VPN network throughput has better QoS while for delay and packet loss on VPN and MPLS VPN networks have the same quality value.

Keywords: *VPN, MPLS VPN, delay, throughput, packet loss.*

1. PENDAHULUAN

Internet yang terus menerus meningkat merupakan tantangan *ISP* (*Internet Service Provider*) untuk masa depan akan kebutuhan lalu lintas jaringan komputer global dan *QoS* (*Quality of service*) yang diharapkan. Internet merupakan sekumpulan jaringan *IP* (*Internet Protocol*) yang bentuk jaringan yang menggunakan protokol *TCP/IP* sebagai protokol utama dalam pembentukan jaringan yang mengantarkan paket dengan memeriksa alamat tujuan *header*. Jika alamat tujuan masih merupakan bagian dalam *network*. paket dihantarkan langsung ke *host* tujuan. Jika alamat tujuan bukan merupakan bagian internal *network*, paket dikirimkan ke *network* lain dengan mekanisme *routing* Jaringan *IP* yang memiliki dua fungsi dasar yaitu pengalamatan dan *fragmentation* memerlukan tiap datagram secara individual dan tidak terkait pada fragmen yang dibuat. Protokol *IP* bekerja dengan mengirimkan paket melalui *rute* yang acak

DOI: 10.34128/jsi.v5i2.191 *Received: October 17th, 2019*
Accepted: November 20th, 2019

tanpa pengirim atau penerima mengetahui jalur perjalanan paket data yang dikirim, Karena bersifat *connectionless*. Paket data tidak dijamin sampai kepada alamat atau datang tepat waktu. Paket data yang dikirim berupa datagram yang merupakan fragmen dari *file* yang dikirim pada jaringan *IP*. Tiap datagram dilepas dalam jaringan komputer dan akan mencari sendiri secara otomatis *rute* yang harus ditempuh ke komputer tujuan. Untuk membentuk *shortest-path* diantara pasangan sumber dan tujuan dengan *routing shortest-path*, trafik dari sumber ke tujuan hanya menggunakan jalur terpendek yang ada sehingga sering terjadi kelebihan kapasitas sementara jalur lain jarang digunakan walaupun jalur itu ada.

Jaringan *VPN* merupakan jaringan komunikasi *private* yang menggunakan jaringan publik untuk membentuk jaringan *Wide Area Network*. *VPN* umumnya didasarkan pada jaringan *IP* yang prinsip dasarnya menggunakan teknologi *tunnel*. *Encapsulating* data dengan protokol *tunnel*, dan membangun *tunnel* berdasarkan jaringan *public* seperti internet untuk menghubungkan titik ke titik. Teknologi *VPN* yang terus menerus berkembang memberikan keuntungan *ISP* dan pelanggan. Teknologi yang diterapkan oleh *ISP* adalah *MPLS VPN* yang menyediakan layanan *VPN* yang melintasi jaringan *MPLS* milik *ISP*. Jaringan *MPLS* (*Multi protocol label switching*) merupakan metode *forwarding* yang meneruskan data melalui suatu jaringan menggunakan informasi dalam label yang diletakan pada paket *IP*. *MPLS* menggabungkan teknologi *switching layer* 2 dengan teknologi *routing layer* 3.

Fitur unik pada *MPLS* adalah memungkinkan seluruh aliran terkendali pada sebuah paket tanpa mengspesifikasi secara eksplisit *router-router* yang dilewati. Hal ini dilakukan dengan membuat *tunnel* yang melewati *router-router* di dalam jaringan *MPLS*. Konsep tersebut digunakan untuk menerapkan *MPLS VPN*. Jaringan *MPLS VPN* muncul sebagai teknologi yang memenuhi persyaratan *VPN* seperti *private IP*, dan kemampuan untuk mendukung alamat yang bertumpuk dalam menyelesaikan masalah kecepatan dan *Quality of Service*. Dengan adanya perbedaan prinsip kerja dari jaringan *VPN* dan *MPLS VPN* maka terdapat perbedaan dari segi *QoS* yang diberikan sehingga perlu dilakukan analisis terhadap *QoS* pada kedua jenis jaringan yang ditawarkan oleh *ISP*.

2. TINJAUAN PUSTAKA

Hasil Penelitian dari *International Journal of Computer Applications* (Grewal & Dangi, 2012) mengenai tradisional *VPN* berbasis *IP* dan *VPN* berbasis *MPLS*. Metode berbasis *MPLS* paket *forwarding* memiliki banyak keuntungan dibandingkan *IP* lapisan *forwarding*. Paket dengan tujuan yang sama tiba pada port yang berbeda dari router dapat ditugaskan untuk berbeda *FEC* (*forwarding equivalence* c*lasses*). *Forwarding* konvensional hanya dapat mempertimbangkan informasi yang bergerak dalam paket. Simulator yang digunakan *NS2*. *VPN IP* untuk *backbone MPLS*, pada tingkat trafik yang berbeda (TR1, TR2, TR3) disimpulkan bahwa *VPN* berkinerja baik ketika kita menggunakan *MPLS*.

Hasil penelitian dari *International Journal of Advanced Research in Computer Engineering & Technology* (Kale & Waichol, 2014) mengenai prilaku protokol *MPLS* dengan *protocol OSPF*, kemudian melakukan analisa atas dasar *throughput*, *packet loss*, *latency* dalam jaringan dengan bantuan *tools* pemantauan jaringan. Dengan menggunakan lima seri *router* Huawei NE20, pengujian dengan *MPLS* dan *IP routing* tradisional, hasilnya menunjukkan penyedia layanan dari *MPLS* dapat meningkatkan *throughput* jaringan dan manfaat diperoleh dari tambahan *MPLS*.

2.1 Jaringan VPN

VPN (*Virtual Private Network*) merupakan sebuah jaringan komunikasi *private* yang menggunakan jaringan publik untuk membentuk suatu jaringan *WAN* (*Wide Area Network*), sehingga dengan cara tersebut seolah–olah pelanggan mendapatkan layanan komunikasi seperti jaringan *private*, namun dengan harga yang lebih efisien (Sasmito, 2012). *VPN* memungkinkan masing-masing *remote user* dari jaringan dapat berkomuikasi dengan jalur yang aman dan dapat diandalkan dengan menggunakan internet sebagai perantara untuk terkoneksi ke *LAN* pribadi. *VPN* dapat dkembangkan untuk mengakomodasi lebih banyak pengguna dan tempat-tempat lain secara lebih mudah daripada *leased line*.

2.2 Jaringan *MPLS VPN*

MPLS VPN yang berfokus pada tautan antara PE (*Provider's Edge router*) dan *CE* (*Costomer's Edge Router*) *router CE* terhubung langsung ke *router PE* sedemikian rupa sehingga lalu lintas data

dienkapsulasi untuk dikirim ke *router-router CE* yang lain. *Router CE* memberitahukan rute-rute *VPN* kepada semua perangkat yang ada dalam jaringan miliknya agar saling terhubung. *MPLS VPN* terdiri dari beberapa site yang saling berhubungan dengan *MPLS provider core network*. Pada setiap *site* terdapat satu atau beberapa *router CE* yang terhubung pada suatu atau beberapa *router PE*. *Router PE* menggunakan *MP-BGP* (*Border Gateway protocol Multiprotocol*) untuk berkomunikasi secara dinamis antara *router PE*. Selama alamat *IP* yang digunakan dalam jaringan *core MPLS VPN* harus eksklusif dan berbeda dengan alamat *IP* yang dimiliki oleh pelanggan *VPN*. Setiap *router CE* harus mampu untuk mengirim paket data ke *router PE* yang berhadapan langsung. Alamat *IP* yang ada pada *router PE* tidak boleh ada yang sama dengan alamat *IP* milik pelanggan *VPN*. *MPLS VPN* yang berbasis *Peer Model*, memiliki skalabilitas yang tinggi, mudah untuk dibangun, dan mudah untuk dimanajemen dibandingkan *VPN* komvensional. *MPLS VPN* memisahkan lalu lintas jaringan dengan *table routing* yang unik, yang disebut *VRFs* (*Virtual Routing Forwading*) pada setiap jaringan *VPN* milik pelanggan. Sehingga setiap pelanggan pada sebuah *VPN* tidak akan bisa melihat lalu lintas jaringan diluar VPN nya. Pemisahan lalu lintas jaringan terjadi tanpa proses tunneling ataupun enkripsi, karena sudah dibangun langsung di dalam jaringan *service provider*.

2.3 *Quality of Service*

Quality of Service (QoS) adalah kemampuan menyediakan jaminan dan performa layanan pada suatu jaringan. Terdapat banyak hal bisa terjadi pada paket ketika melakukan perjalanan dari sumber ke tujuan, masalah-masalah tersebut meliputi *delay*, *throughput*, dan *packet loss* (Aryanta, 2013).

2.3.1 *Delay*

Deley atau *Latency* adalah berapa lama waktu yang dibutuhkan seluruh pesan untuk benar-benar tiba di tujuan dari waktu bit pertama dikirim keluar dari sumbernya (Forouzan, 2007). Untuk dapat mengetahui kualitas dari nilai *delay* dapat digunakan standar TIPHON seperti ditujukan pada Tabel 1 (ETSI, 1999).

Tabel 1. Standar Kualitas *Delay*

Kategori	*Delay* (ms)	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300	3
Sedang	300 s/d 450	2
Jelek	> 450	1

Untuk dapat mencari nilai *delay* dapat digunakan persamaan (1) sebagai berikut:

$$Delay = \frac{Packet\ Length}{Link\ Bandwidth} \quad (1)$$

2.3.2 *Throughput*

Throughput adalah kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* dikaitkan dengan *bandwidth*. Karena *throughput* memang bisa disebut dengan *bandwidth* dalam kondisi yang sebenarnya. Sementara *throughput* sifatnya adalah dinamis tergantung trafik yang sedang terjadi. Semakin besar nilai *throughput* nya akan menunjukkan semakin bagus pula kemampuan jaringan dalam mentransmisikan file. Nilai *throughput* sesuai dengan *telkom polytechnic quality standarts throughput* (Sugeng, Istiyanto, Mustofa, & Ashari, 2015) seperti ditujukan pada Tabel 2.

Tabel 2. Standar Kualitas *throughput*

Kategori	*throughput* (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	< 25	1

Untuk dapat mencari nilai *throughput* dapat digunakan persamaan (2) sebagai berikut:

$$Throughput = \frac{\sum data\ yang\ dikirim\ (bit)}{Waktu\ Pengiriman\ Data}\ bps \quad (2)$$

2.3.3 *Packet Loss*

Packet Loss merupakan banyaknya paket yang gagal untuk mencapai tempat tujuan pada saat paket tersebut dikirim. Ketika packet loss besar maka dapat diketahui bahwa jaringan sedang sibuk atau terjadi *overload. Packet loss* mempengaruhi kinerja jaringan secara langsung. Nilai *packet loss* sesuai dengan versi *ETSI TIPHON* yang ditujukan pada Tabel 3 (ETSI, 1999).

Tabel 3. Standar *Packet loss*

Kategori	*Packet loss* (%)	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	1

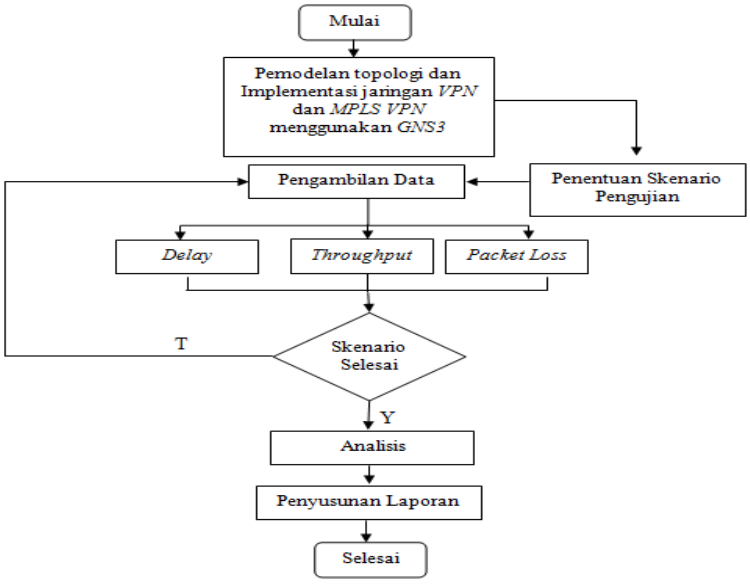
Untuk dapat mencari nilai *packet loss* dapat digunakan persamaan (3) sebagai berikut:

$$Packet\ loss = \frac{Paket\ data\ dikirim - Paket\ data\ diterima}{Paket\ data\ yang\ dikirim} x100\ \% \quad (3)$$

3. METODE PENELITIAN

3.1 Tahapan Penelitian

Pada penelitian ini, analisis *QoS* pada jaringan *VPN* dan *MPLS VPN* menggunakan metode riset eksperimental. Riset eksperimental merupakan penelitian yang memungkinkan untuk menentukan penyebab dari suatu perilaku. Untuk menggambarkan riset eksperimental bisa dilakukan pada dua kelompok dimana kelompok satu disebut kontrol tanpa diberi perlakukan apapun sedangkan pada kelompok ke dua diberikan perlakuan (*treatment*). Diasumsikan kedua kelompok ini sama. Adapun tahapan penelitian yang dilakukan dapat dilihat pada Gambar 1.



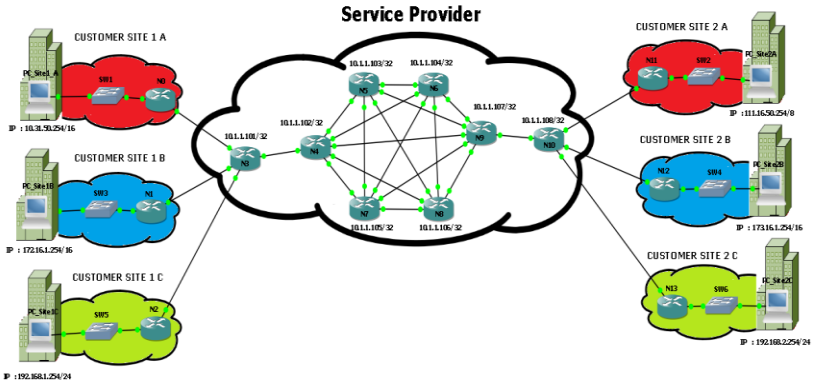
Gambar 1. Tahapan penelitian penelitian

3.2 Rancangan Topologi jaringan

Perancangan model topologi jaringan merupakan hal utama yang dibutuhkan seorang *network administrator* dalam membangun sebuah simulasi jaringan. Simulasi jaringan dibangun untuk melihat kebutuhan suatu jaringan. Dalam hal ini *network administrator* dapat mengkoordinasi dan melakukan *management network*. Berikut ini merupakan sebuah perancangan topologi

p-ISSN: 2460-173X
e-ISSN: 2598-5841

jaringan *VPN* dan jaringan *MPLS VPN*. Topologi tersebut terhubung dalam bentuk *full mash*. Adapun topologi yang akan dimplementasikan seperti yang ditujukan pada Gambar 2.



Gambar 2. Simulasi jaringan secara umum

Gambar 2 menjelaskanTopologi yang akan digunakan untuk mensimulasikan Jaringan *VPN* dan jaringan *MPLS VPN* yang mengambarkan kondisi jaringan dengan *bandwith* untuk *link* adalah 100 Mbps kecuali untuk *link node* N0-PC_site1A dan N11-PC_site2a yaitu 128 Kbps, N1-Pc_Site1B dan N12-Pc_site2B yaitu 256 Kbps serta N2-PC_Site1C dan N13-PC-Site2C yaitu 512 Kbps. Adapun topologi tersebut terdiri dari 13 *node* yang terhubung dengan bentuk *full mash*.

3.3 Rancangan Implementasi

Tahapan implementasi jaringan *VPN* dan jaringan *MPLS VPN* dilakukan dengan melakukan konfigurasi pada *router* milik Cisco menggunakan simulator *GNS3* konfigurasi adalah sebagai berikut:

3.3.1 Konfigurasi Jaringan *VPN*

- Konfigurasi untuk semua *interface router* yang terhubung ke beberapa *port* dengan memberikan alamat *IP* untuk masing-masing *port* yang terhubung ke *router*.
- Konfigurasi *VPN server* dilakukan pada sisi *router* N0, N1, dan N2 yang berfungsi sebagai *router server* dikonfigurasi dengan menggunakan protokol *tunneling L2TP server*
- Konfigurasi *VPN Client* dilakukan pada sisi *router* N11, N12, dan N13 yang berfungsi sebagai *router client* dengan dikonfigurasi dengan menggunakan Protokol *Tunneling L2TP Client.*

3.3.2 Konfigurasi Jaringan *MPLS VPN*

- Konfigurasi untuk semua *interface router* yang terhubung ke beberapa *port* dengan memberikan alamat *IP* untuk masing-masing *port* yang terhubung ke *router*
- Konfigurasi *MPLS* dilakukan ke semua *router*, konfigurasi tersebut untuk membangun *LSP* pada area *MPLS* agar dapat memberikan label pada paket data *IP* yang melewati *path* tersebut.
- Konfigurasi *MPLS VPN* dilakukan pada *router* N3 sebagai *ingress LER* dan N10 sebagai *Engress LER* menggunakan *VRF* untuk membangun *MPLS VPN layer* 3.

3.4 Rancangan Skenario Pengujian

Proses pengujian dilakukan dengan 3 kali pengambilan data. Untuk ukuran file yang di uji sebesar 102 KB, 220 KB, 412 KB 1.16 MB, 2,08 MB, 4,18 MB, 8,07 MB dan 10.0 MB. Parameter *QoS* yang ingin diamati adalah nilai dari *delay, packet loss, dan throughput*. Berikut adalah skenario pengujian yang ditujukan pada Tabel 4.

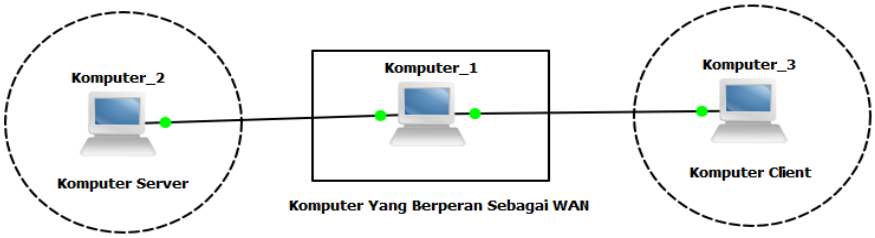
Tabel 4. Rancangan skenario pengujian

Skenario	Client	*Ukuran Bandwidth (Kbps)*	*Nama Trafik*
Skenario I	CE_VPN2A ke CE_VPN1A	128	FTP0
Skenario II	CE_VPN2B ke CE_VPN1B	256	FTP1
Skenario III	CE_VPN2C ke CE_VPN1C	512	FTP2

4. PEMBAHASAN

4.1 Perancangan Simulasi Jaringan

Untuk mensimulasikan jaringan *VPN* dan *MPLS VPN* diperlukan 3 buah komputer. Komputer 1 yang didalamnya terdapat konfigurasi topologi *full mesh* seperti terlihat pada Gambar 2 yang berperan sebagai router *WAN*, komputer 2 berperan sebagai server yang didalamnya terdapat aplikasi core FTP server, dan komputer 3 berperan sebagai client yang didalamnya terdapat aplikasi Filezilla FTP client dan aplikasi wireshark untuk menagkap paket data. Komputer 2 dan 3 dihubungkan langsung ke komputer 1 dengan kabel *UTP* dalam bantuk *cross-over* seperti yang terlihat pada Gambar 3.



Gambar 3. Model topologi simulasi

Pada Gambar 3 menunjukan model simulasi yang dilakukan dengan spesifikasi komputer 1 memiliki 2 buah NIC 10 Mbps dengan RAM 2 GB dan processor Intel Core i3, untuk komputer 2 memiliki NIC 10 Mbps dengan RAM 2 GB dengan processor Intel Core i3. Dan untuk komputer 3 memiliki processor AMD Dual Core c60, RAM 2 GB dengan NIC 10 Mbps.

4.2 Implementasi

4.2.1 Konfigurasi Jaringan *VPN*

Konfigurasi protokol *tunnel L2TP* pada jaringan dilakukan pada router router PE di customer. Berikut adalah konfigurasi protocol *Tunnel L2TP* di router N3.

```
N3(config)#Pseudowire-class PW_MANUAL
N3(config-pw-class)#encapsulation L2tpv3
N3(config-pw-class)#Protocol None
N3(config-pw-class)#ip local inteface Loopback0
N3(config)#interface F0/0
N3(config-if)#bandwidth 128
N3(config-if)#no shutdown
N3(config-if)#xconnect 134.8.1.108 33 encapsulation l2tpv3 manual pw-class PW_MANUAL
N3(config-if)#l2tp id 245 329
N3(config-if)#l2tp cookie local 8 957344 9379092
N3(config-if)#l2tp cookie remote 8 76429 945
N3(config)#Interface F0/1
N3(config-if)#bandwidth 256
N3(config-if)# no shutdown
N3(config-if)#xconnect 134.8.1.108 34 encapsulation l2tpv3 manual pw-class PW_MANUAL
N3(config-if)#l2tp id 345 429
N3(config-if)#l2tp cookie local 8 947444 9279092
N3(config-if)#l2tp cookie remote 8 75319 935
N3(config)#Interface F1/0
N3(config-if)#bandwidth 512
N3(config-if)# no shutdown
N3(config-if)#xconnect 134.8.1.108 35 encapsulation l2tpv3 manual pw-class PW_MANUAL
N3(config-if)#l2tp id 445 529
N3(config-if)#l2tp cookie local 8 937544 9179092
N3(config-if)#l2tp cookie remote 8 74209 925
```

Pada konfigurasi diatas, router N3 berfungsi untuk menghubungkan customer pusat Perintah "*Pseudowire-class*" yang digunakan untuk membangun saluran yang dilewati diatas jaringan *L2TPv3* pada router *ISP* dengan nama yang diberikan adalah "PW_MANUAL". Pada router N3 yang menghubungkan cutomer pusat digunakan perintah "*xconnect*" dengan *loopback address* 134.8.1.108 yang mengarah ke router N10 milik customer cabang. Hal tersebut digunakan untuk membangun *peer address*. Sedangkan untuk nilai 33, 34 dan 35 digunakan untuk membangun *virtual circuits ID* (VCID) pada masing-masing customer. *VCID* di identifikasikan secara unik untuk melampirkan circuit berbasis *peer-to-peer*. setelah mengkonfigurasi *xconnect submode* maka diperlukan secara manual untuk

mendefinisikan atribut dari *session id, Cookie Local* dan *Cookie* Remote nilai tersebut di berikan secara perspektiv untuk *Session ID, Cookie Local,* dan *Cookie Remote*. Untuk *remote ID*= 329, 429, dan 529 router N3 diatas, akan dikonfigurasi pada router N10 menjadi *Local ID* =329, 429 dan 529 sedangkan untuk *Local Id* di router N3 dikonfigurasi menjadi *Remote ID*= 245, 345, dan 445 pada router N10. Hal ini dilakukan untuk membangun *virtual circuit* berbasis *Peer-to-peer* pada masing-masing customer pelanggan *VPN* di *service provider*. Berikut adalah konfigurasi *Protocol Tunnel L2TP* di router N10:

```
N10(config)#Pseudowire-class PW_MANUAL
N10(config-pw-class)#encapsulation L2tpv3
N10(config-pw-class)#Protocol None
N10(config-pw-class)#IP local interface Loopback0
N10(config-pw-class)#exit
N10(config)#interface F0/0
N10(config-if)#no shutdown
N10(config-if)#xconnect 134.1.1.101 33 encapsulation l2tpv3 manual pw-class PW_MANUAL
N10(config-if)#l2tp id 329 245
N10(config-if)#l2tp cookie local 8 76429 945
N10(config-if)#l2tp cookie remote 8 957344 9379092
N10(config-if)#exit
N10(config)#Interface F1/0
N10(config-if)# no shutdown
N10(config-if)#xconnect 134.1.1.101 34 encapsulation l2tpv3 manual pw-class PW_MANUAL
N10(config-if)#l2tp id 429 345
N10(config-if)#l2tp cookie local 8 75319 935
N10(config-if)#l2tp cookie remote 8 947444 9279092
N10(config-if)#exit
N10(config)#Interface F1/1
N10(config-if)# no shutdown
N10(config-if)#xconnect 134.1.1.101 35 encapsulation l2tpv3 manual pw-class PW_MANUAL
N10(config-if)#l2tp id 529 445
N10(config-if)#l2tp cookie local 8 74209 925
N10(config-if)#l2tp cookie remote 8 937544 9179092
N10(config-if)#exit
```

Konfigurasi *Protocol Tunnel L2TP* diatas, pada router N10 perintah "*xconnect"* yang *looback address* 134.1.1.101 yang mengarah ke router PE yang menghubungkan customer pusat. dikonfigurasi pada *session id, Cookie Local* dan *Cookie Remote* dilakukan secara *cross*.

4.2.2 Konfigurasi Jaringan *MPLS-VPN*

Agar MPLS aktif di router *core* dan *PE*, maka seluruh *interface* yang menerapkan label MPLS di jaringan service provider diaktifkan. Berikut adalah konfigurasi untuk mengaktifkan MPLS di jaringan router Core1:

```
Core1(config)#interface F0/0
Core1(config-if)#mpls ip
Core1(config)#exit
Core1(config)#interface F0/1
Core1(config-if)#mpls ip
Core1(config)#exit
Core1(config)#interface F1/0
Core1(config-if)#mpls ip
Core1(config)#exit
```

```
Core1(config)#interface F1/1
Core1(config-if)#mpls ip
Core1(config)#exit
Core1(config)#interface F2/0
Core1(config-if#mpls ip
Core1(config)#exit
Core1(config)#interface F2/1
Core1(config-ip)#mpls ip
Core1(config)#exit
```

Pada router core semua *interface* harus diaktifkan *MPLS ip* karena semua router core menuju router *PE* yang harus menerakan label *MPLS* sedangkan ntuk router *PE mpls ip* diterapkan ke *interface* yang menuju ke *router core* dalam jaringan *provider*. Untuk pengecekan apakah *MPLS* sudah aktif dan berjalan dengan baik, digunakan perintah" *show mpls forwarding-table*" pada *previledge mode*. Jika sudah terbentuk maka akan terlihat *PE* akan mengenal core sebagai router *MPLS*.

VRF (*Virtual router Forwarding*) digunakan untuk setiap *CE*. virtual *router* tersebut dibuat di masing-masing *customer* yang seolah-olah memiliki *router* sendiri yang dapat mengatur trafik mereka melalui *MPLS* domanin. Untuk masing-masing *VRF customer* memiliki identitas sendiri-sendiri dikarenakan hal tersebut dapat memungkinkan *customer* yang berbeda namun memiliki *IP address* yang sama dapat diakomodir menggunakan *MPLS network*. Pada *PE1* dan *PE2* terdapat *3 VRF* yaitu *VPN1*, *VPN2*, dan *VPN3*. Untuk membuat router virtual pada router PE1 dan PE2 dilakukan konfigurasi *VRF*. Berikut adalah Konfigurasi *VRF* di router PE1dan PE2:

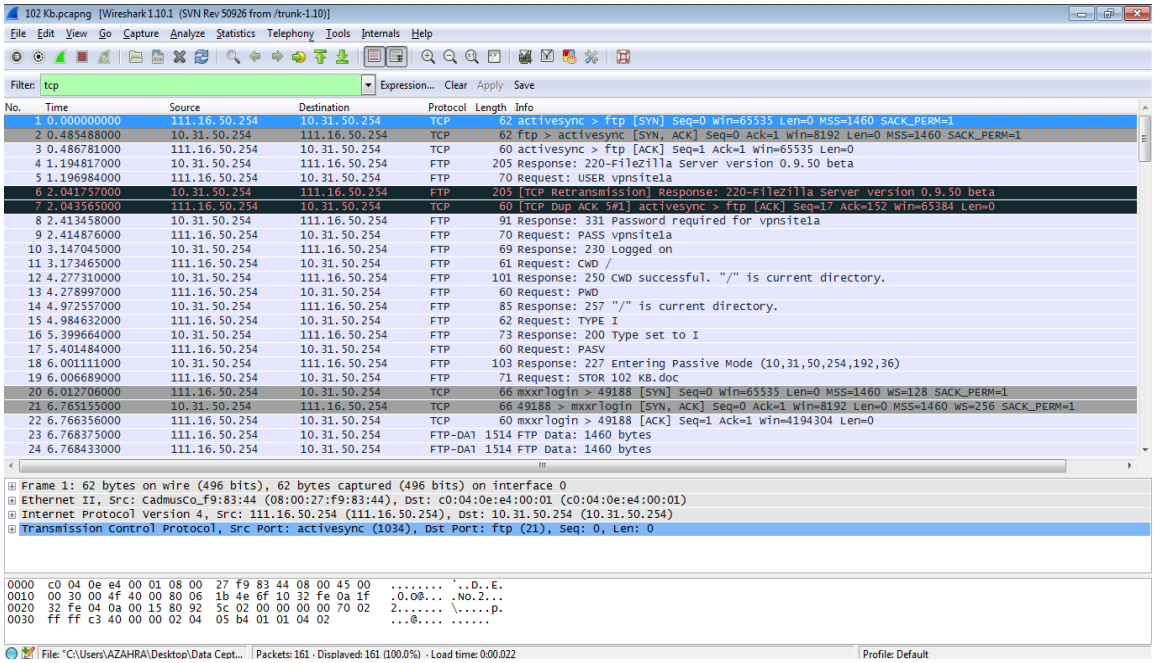
```
PE2(config)#ip vrf vpn1
PE2(config-vrf)#rd 1:10
PE2(config-vrf)#route-target export 1:10
PE2(config-vrf)#route-target import 1:10
PE2(config)#ip vrf vpn2
PE2(config-vrf)#rd 2:20
```

```
PE2(config-vrf)#route-target export 2:20
PE2(config-vrf)#route-target import 2:20
PE2(config)#ip vrf vpn3
PE2(config-vrf)#rd 3:30
PE2(config-vrf)#route-target export 3:30
PE2(config-vrf)#route-target import 3:30
```

Konfigurasi *CLI* diatas, terlihat bahwa RD (*Router Distinguisher*) yang merupakan identitas dari sebuah *VRF* pada setiap *customer* sedangkan *route-target* digunakan untuk menentukan *route* yang akan *import* ke dalam *VRF* dan menenentukan *Route* yang akan di *export*. Pada *route-target export* di PE1 menyatakan bahwa semua *routing table* atau *routing prefix* di router virtual *VRF VPN1*, jika akan dikirim ke PE2, maka akan diberi tanda dengan RD 1:10 *routing perfix* tersebut setelah sampai di PE2 akan digunakan dengan mengimport terlebih dahulu *route* dengan RD 1:10. Itulah untuk *routing customer site* 1 A sedangkan untuk *routing* customer site 1 B menggunakan RD 2:20 dan *routing* customer site 1 C menggunakan RD 3:30. Untuk nama dari VPN1, VPN2 dan VPN3 tersebut berlaku secara local di router PE nomor RD tersebut akan dipertukarkan antara PE.

4.3. Pengambilan Data

Setelah melakukan konfigurasi maka dilakukan beberapa uji simulasi dan pengambilan data pada jaringan *VPN* dan *MPLS VPN* yang dibuat dapat berjalan dengan baik di GNS3 menggunakan 3 buah komputer dan aplikasi *wireshark* untuk menagkap aliran data *FTP*. Untuk dapat melakukan pengiriman data digunakan aplikasi core *FTP server* dan filezilla *FTP* client sedangkan untuk melakukan filter tarhadap data yang diunduh dari client ke server dilakukan filter data pada *protocol TCP*, hal ini dikarenakan pada lapisan *TCP/IP* aplikasi *FTP* yang yang menjadi agent untuk memecah data dalam bentuk paket-paket yang lebih kecil agar mudah untuk dikirim. Berikut adalah hasil penagkapan paket data yang ditujukan pada Gambar 4.



Gambar 4. Hasil penangkapan paket data *FTP*

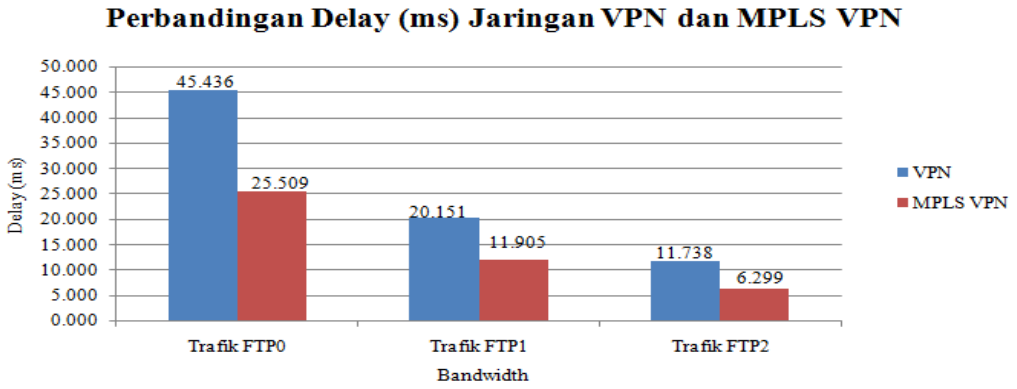
Berdasasrkan data yang telah diambi, pengolahan data dilakukan dengan dengan melakukan perbandingan antara jaringan *VPN* dan *MPLS VPN*. Parameter yang dibandingkan adalah *delay, throughput,* dan *packet loss* sehingga dapat diketahui QoS jaringan yang lebih baik.

4.2.3 Perbandingan *Delay* Jaringan *VPN* dan *MPLS VPN*

Analisis hasil perbandingan *delay* dilakukan berdasarkan nilai hasil rata-rata *delay* dari 3 kali percobaan tanpa melibatkan *backround traffic*. Dari hasil rata-rata *delay* jaringan *VPN* dan *MPLS VPN*

p-ISSN: 2460-173X
e-ISSN: 2598-5841

untuk mencapai keputusan dari perbandingan digunakan standar TIPHON. Berikut adalah hasil perbandingan *delay* jaringan *VPN* dan *MPLS VPN* yang dapat dilihat pada Gambar 5.

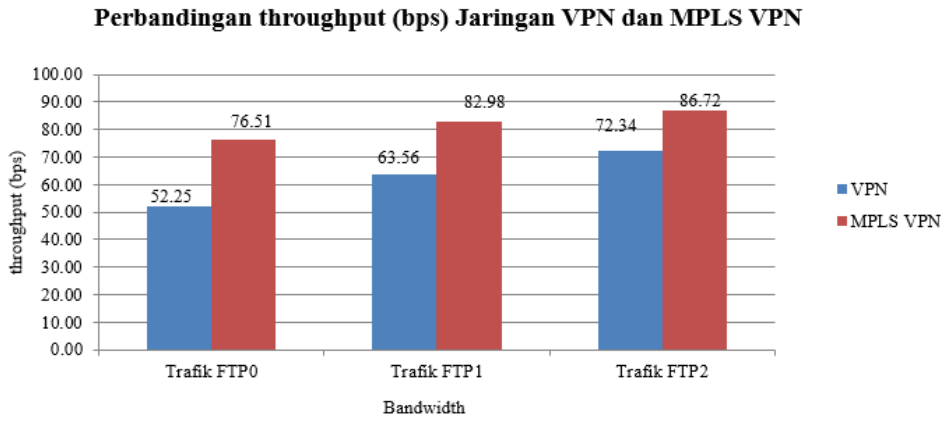


Gambar 5. Grafik perbandingan *delay* jaringan *VPN* dan *MPLS VPN*

Dari hasil pengukuran dapat dilihat pada jaringan *VPN* dan *MPLS VPN* memiliki perbandingan *delay* yang terdapat dari jaringan *VPN* dengan nama trafik FTP0 45,436 ms, FTP1 20,151 ms, dan FTP2 11,738 ms. Sedangkan *delay* yang dihasilkan jaringan *MPLS VPN* dengan nama trafik FTP0 25,509 ms, FTP1 11,905 ms, dan FTP2 6,299 ms. dari data tersebut dapat dilihat bahwa jaringan *MPLS VPN* memilik nilai *delay* yang lebih kecil dari semua jenis trafik yang diuji akan tetapi kedua jaringan tersebut masih memenuhi standar TIPON yaitu dibawah 150 ms. Dari hasil pengukuran dapat dianalisis bahwa pada jaringan *MPLS VPN* dapat memperpendek proses routing dalam pengiriman paket sehingga paket data akan cepat sampai ke tujuan.

4.4 Perbandingan Throughput Jaringan *VPN* dan *MPLS VPN*

Analisis hasil perbandingan *throughput* dilakukan berdasarkan nilai hasil rata-rata dari 3 kali percobaan tanpa melibatkan *backround traffic*. Dari hasil rata-rata *throughput* jaringan *VPN* dan *MPLS VPN* untuk mencapai keputusan dari perbandingan digunakan standar *telkom polytechnic quality standarts throunghput*. Berikut adalah hasil perbandingan *throughput* jaringan *VPN* dan *MPLS VPN* yang terlihat pada Gambar 6.



Gambar 6. Grafik perbandingan *throughput* jaringan *VPN* dan *MPLS VPN*

Dari hasil pengukuran *throughput* pada *VPN* dengan nama trafik FTP0 52.25 bps, trafik FTP1 63.56 bps, dan trafik FTP2 72.34 bps dengan kualitas *throughput* Sedang. Sedangkan pada jaringan *MPLS VPN* dengan nama trafik yaitu FTP0 76.51 bps, FTP1 82.98 bps, dan FTP2 86.72 bps dengan kualitas *throughput* Bagus. Dengan demikian *MPLS VPN* memiliki *throughput* yang stabil sehingga jaringan *MPLS VPN* dapat mendukung *QoS* yang lebih baik dibandingkan dengan jaringan *VPN*.

4.5 Perbandingan *Packet Loss* Jaringan *VPN* dan *MPLS VPN*

Perbandingan *packet loss* pada jaringan *VPN* dan *MPLS VPN* tidak memiliki *packet loss*. Dalam hal *packet loss* pada jaringan *VPN* dan *MPLS VPN* 0 % dengan demikian kualitas layanan sangat bagus. hal ini diakibatkan apabila terjadi kehilangan paket penerima akan meminta *retransmission* atau pengiriman secara otomatis *resends* sehingga tidak diperoleh kehilangan paket.

5. KESIMPULAN

Dari hasil analisis dan pengujian *QoS* pada jaringan *VPN* dan *MPLS VPN* yang telah dilakukan, dapat disimpulkan sebagai berikut:

1. Perbandingan *delay* dari jaringan *VPN* dengan nama trafik FTP0 45,436 ms, FTP1 20,151 ms, dan FTP2 11,738 ms. Sedangkan *delay* yang dihasilkan jaringan *MPLS VPN* dengan nama trafik FTP0 25,509 ms, FTP1 11,905 ms, dan FTP2 6,299 ms. dari data tersebut dapat dilihat bahwa jaringan *VPN* dan *MPLS VPN* memilik nilai *delay* sangat bagus. Akan tetapi pada jaringan *MPLS VPN* dapat memperpendek proses *routing* dalam pengiriman paket sehingga paket data akan cepat sampai ke tujuan dibandingkan dengan jaringan *VPN*.
2. Perbandingan *throughput* pada *VPN* pada trafik FTP0 52.25 bps, trafik FTP1 63.56 bps, dan trafik FTP2 72.34 bps dengan kualitas *throughput* Sedang. Sedangkan pada jaringan *MPLS VPN* dengan nama trafik yaitu FTP0 76.51 bps, FTP1 82.98 bps, dan FTP2 86.72 bps dengan kualitas *throughput* Bagus. Dengan demikian *MPLS VPN* memiliki *throughput* yang stabil sehingga jaringan *MPLS VPN* dapat mendukung *QoS* lebih baik dibandingkan dengan jaringan *VPN*.
3. Perbandingan *packet loss* pada jaringan *VPN* dan *MPLS VPN* tidak memiliki *packet loss*. Dalam hal *packet loss* pada jaringan *VPN* dan *MPLS VPN* 0 % dengan demikian kualitas layanan sangat bagus. hal ini diakibatkan apabila terjadi kehilangan paket penerima akan meminta *retransmission* atau pengiriman secara otomatis *resends* sehingga tidak diperoleh kehilangan paket.

DAFTAR PUSTAKA

Aryanta, D. (2013). Analisis Perbandingan Kinerja Layanan Triple Play pada Jaringan IP dan MPLS Menggunakan NS2. *Jurnal Informatika Itenas*, *4*(1), 25–37.

ETSI. (1999). *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)*. Valbonne.

Forouzan, B. A. (2007). *Data Communications and Networking, Fourth Edition*. United States: McGraw-Hill Companies Inc.

Grewal, K., & Dangi, R. (2012). Comparative Analysis of QoS VPN Provisioning Algorithm on Traditional IP based VPN and MPLS VPN using NS-2. *International Journal of Computer Applications*, *48*(1), 43–46. https://doi.org/10.5120/7316-9922

Kale, N. N., & Waichol, S. A. (2014). Performance Analysis of MPLS network with Traditional IP Network in Service Provider Environment. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *3*(4), 1311–1316.

Sasmito, E. C. (2012). Produk & Layanan IPVPN MPLS. Retrieved November 4, 2014, from https://ekocandrasasmito.wordpress.com/2012/06/09/produk-layanan-ipvpn-mpls/

Sugeng, W., Istiyanto, J. E., Mustofa, K., & Ashari, A. (2015). The Impact of QoS Changes towards Network Performance. *International Jurnal of Computer Networks and Communications Security*, *3*(2), 48–53.

Biodata Penulis

Mardianto, lahir di wundulako pada tanggal 17 Desember 1988. meraih gelar Sarjana komputer (S.Kom) dari Universitas Sembilanbelas November kolaka dan menyelesaikan program Magister Computer Science (M.Cs) pada Program Studi Ilmu komputer Universitas Gadjah mada.