OPEN ACCESS
J. OF ICT, VOL. 2, NO. 2, PP.049-056, DES 2020
ISSN : 2686-1089 (ONLINE)

Journal of Informatics and Communications Technology (JICT)

Tunneling Pipe Mode Pada Jaringan Multi Protocol Label Switching

Ananda Esa Putra Sunarto [#1], Ade Nurhayati [*2]

#[1,2] *Akademi Teknik Telekomunikasi Sandhy Putra Jakarta, First-second Jl Daan Mogot KM 11 Jakarta Barat*

[1] anandaesaap@gmail.com
[2] adenurhayati@akademitelkom.ac.id

Abstract

Along with the developing and the increasing of data communication users, service providers are required to always improve the quality of their services. QoS plays an important role since it is a parameter of the quality level of a service. Pipe Tunneling technique is one of the Qos methods that will guarantee a service will have its own priority level. With the help of the MPLS-VPN protocol, addressing of the IP will be much more flexible. In this thesis the simulation was done using GNS3 software while the results of the analysis were carried out using the WireShark software. There are two scenarios done by the author. For MPLS-VPN the author simulates 2 customers between companies 1 and 2 where both companies have centers in Jakarta and branches in Surabaya. And for Tunneling, both companies want their services to be given the highest priority among other services. From this scenario it can be obtained that with the presence of VRF on the network if there is the same network usage there will be no overlaps of IP. A service will have its own priority level according to the needs and requests. The results of the analysis are more focused on QoS, especially delay and throughput. From the results it shows that MPLS-VPN with Tunneling Pipe Mode integration is able to keep good QoS value. This can be seen from the average of the delay and throughput yield for Tunneling Pipe Mode that is equal to 84,51 ms and 67,858 Bytes / s.

Keywords: MPLS, VPN, Routing, TunnelingMode, QoS

I. INTRODUCTION

Banyaknya perusahaan atau organisasi yang mendaftarkan kelompoknya ke ISP membuat daftar alamat IP yang ada di ISP semakin menumpuk. Hal ini dapat membuat resiko terjadinya overlap ip dimana terdapat pemakaian dua ip network yang sama dalam satu waktu yang dapat menyebabkan terjadinya kegagalan koneksi. Di samping itu, setiap perusahaan atau organisasi tersebut tentunya memiliki permintaan masing – masing yang mengharuskan ISPuntuk mengikuti semua permintaan yang diminta, seperti perusahaan tersebut meminta ISP untuk memberikan prioritas untuk layanannya dibandingkan dengan layanan – layanan untuk perusahaan lainnya. Untuk mengatasi semua masalah tersebut digunakanlah sebuah metode Virtual Routing Forwarding (VRF) yang diintegrasikan dengan protokol Multi Protocol Label Switching (MPLS) yang dapat mengizinkan pemakaian ip network secara bersamaan. Disamping itu, metode Tunneling Pipe Mode digunakan untuk memberikan prioritas kepada masing – masing layanan untuk perusahaan yang memintanya dengan hasil QoS yang diharapkan.

II. LITERATURE REVIEW

Penelitian ini mengacu pada penelitian sebelumnya yaitu '*Hybrid evolutionary MPLS Tunneling Algorithm based on high priority bits'*. Pada penelitian ini tunneling MPLS menggunakan Hybrid MPLS Tunneling

Algorithm (HMTA) yang meliputi Teknik Differensiasi Bandwidth dan Delay serta penentuan bit prioritas pada setiap data paket dengan tujuan memperbaiki QoS routing dari jaringan MPLS. [1]

Pada penelitian ini akan dibahas tunneling pada Differential Service dengan simulasi tunneling yaitu pipe mode pada jaringan MPLS-VPN (Multi Protocol Label Switching-Virtual Private Network). Tunneling pipe mode dilakukan dengan memberikan prioritas terhadap layanan tertentu pada layanan MPLS-VPN.

MPLS (Multi Protocol Label Switching) merupakan sebuah teknologi transmisi paket data pada jalur backbone berkecepatan tinggi. Pada umumnya, MPLS banyak digunakan saat membangun suatu jaringan yang sifatnya tertutup yang menghubungkan kantor pusat di suatu kota dengan kantor – kantor cabangnya yang berada di kota – kota lain melalui sebuah link yang berkecepatan tinggi. [2]. MPLS-VPN terdiri dari :

1. Core / Provider – router ISP yang tidak terhubung dengan customer secara langsung tetapi terhubung dengan PE, di Router ini hanya mengemban MPLS dan tidak memberi label VPN.
2. PE (Provider Edge) – router ISP yang terhubung dengan customer,di router inilah labelVPN dibuat dan diberi pada data.
3. CE(Customer Edge) – router milik pelanggan yang terhubung dengan ISP

Dalam hal meningkatkan performansi QoS, Differential Service (Diffserv) dapat digunakan sebagai salah satu pilihan untuk layanan QoS nya. Caranya yaitu dengan menggunakan pengaturan kode layanan terdiferensiasi 6-bit Differentiated Services Code Point (DSCP) atau IP Precedence dalam paket IP atau alamat sumber dan tujuan[5]. Ada dua jenis Tunneling Mode pada Diffserv. Tunneling Mode sendiri merupakan ekstensi dari model Diffserv (Differentiated Service) yang dapat menawarkan kualitas layanan jaringan dan dapat memberikan proritas ke setiap layanan yang ingin diberikan. Jenis – jenis Tunneling Mode pada Diffserv yaitu :

1. Uniform Mode

Mode Tunneling ini biasanya digunakan apabila antara penyedia layanan dan pelanggan sama – sama memiliki domain yang sama. Prinsipnya menggunakan IP Precedence atau DSCP Code Point pada saat pengiriman informasi. [5]

2. Pipe Mode

Mode Tunneling ini biasanya digunakan ketika terdapat router customer edge (CE) yang terkelola dengan baik yang artinya jaringan yang menggunakan mode ini jaringan berskala besar.Prinsipnya menggunakan MPLS EXPERIMENTAL bits pada saat pengiriman informasi. [5]

Quality of Service yang akan diukur dalam penelitian ini antara lain :

1. Delay

Delay adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari suatu node ke node lain yang menjadi tujuannya [7]. Standar parameter yang digunakan adalah berdasarkan THIPON sebagai berikut :

Tabel 1. Standar Delay Thippon

KATEGORI	BESAR DELAY
Sangat Bagus	< 150 ms
Bagus	< 250 ms
Sedang	< 350 ms
Buruk	< 450 ms

2. Troughput

Throughput adalah presentase jumlah paket yang sukses di transmisikan yang merupakan perbandingan jumlah paket yang sukses dikirim dengan jumlah paket yang ditransmisikan. Karena sejumlah faktor, Throughput biasanya tidak sesuai dengan bandwidth yang ditentukan dalam implementasi lapisan fisik seperti Ethernet[7]. Standar parameter Troughput berdasarkan THIPON sebagai berikut :

Tabel 2. Standar Troughput Thippon

KATEGORI	THROUGHPUT
Sangat bagus	5-100
Bagus	0-75
Sedang	5-50
Buruk	25

Untuk mengethaui kinerja dari tunneling pipe mode dilakukan dengan simulasi menggunakan GNS3 (Generator Network Simulation 3) yaitu simulator grafis yang bersifat emulator, sementara pengukuran performansinya sendiri menggunakan wireshark yang merupakan tools network analyzer.

III. RESEARCH METHOD

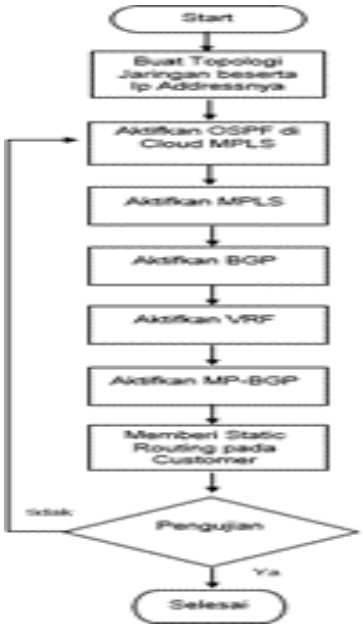
Penelitian ini dilakukan dengan proses simulasi menggunakan simulator GNS3. Berikut adalah software yang digunakan untuk simulasi :

Tabel 3. Daftar Software Simulasi

No	Daftar Software	
	Aplikasi	**Jenis / Versi**
1.	GNS3	*Version*2.1.5
2.	*Image* GNS3	*c7200-advipservicesk9-mz.152-4.S5.image*
3.	*Wireshark*	*Version 2.2.7*
4.	*Windows 10*	*Home*
5.	*VirtualBox* (optional)	*Version* 5.2.12

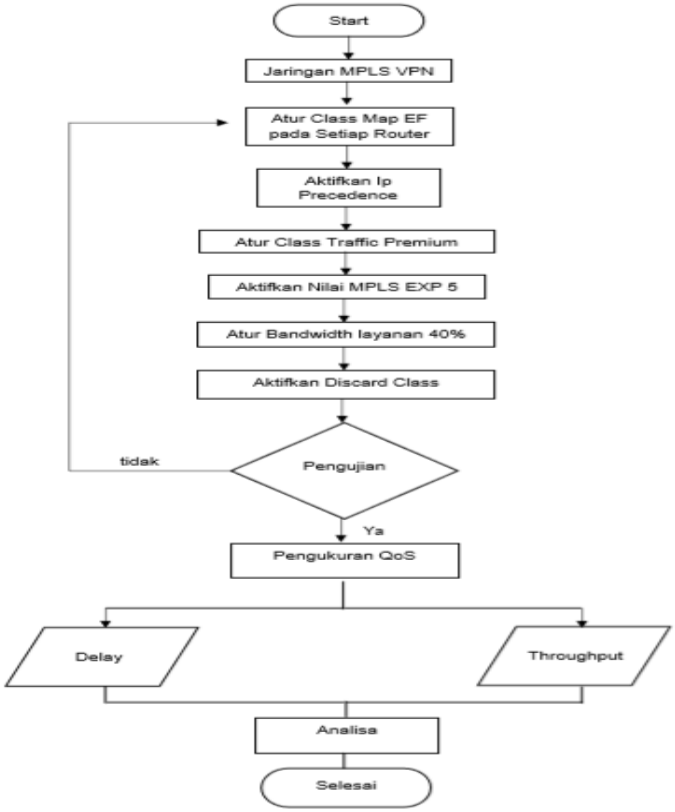
A. Diagram Alur Penelitian

Dalam pelaksanaan penelitian, penulis melakukan beberapa langkah yang tercantum dalam diagram alir berikut :



Gambar 1. Diagram alir Proses Penelitian

Untuk proses konfigurasinya sendiri berdasarkan diagram alir berikut ini :



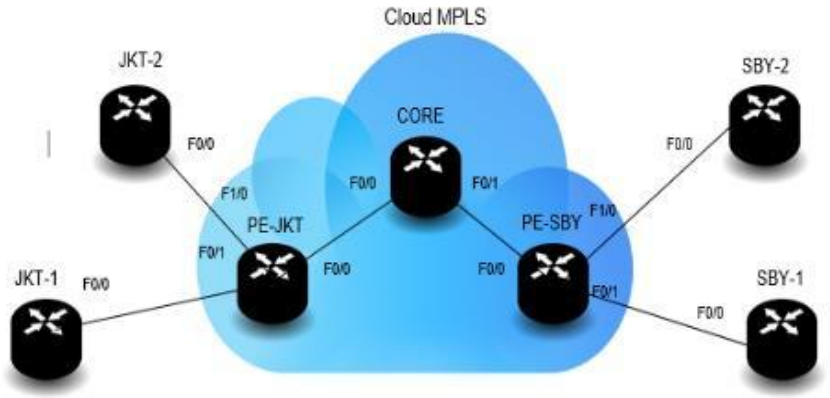
Gambar 2. Diagram Alir Konfigurasi Tunneling

Proses simulasi :

1. Instalasi software simulator GNS3 dan menambahkan IOS image router cisco ke dalam GNS3.
2. Membuat topologi MPLS-VPN
3. Melakukan konfigurasi demi konfigurasi untuk membangun jaringan MPLS-VPN.
4. Melakukan konfigurasi untuk metode Diffserv Pipe Mode Tunneling.
5. Menguji simulasi jaringan tersebut dan mengukur Delay dan Throughput yang dihasilkan.

B. Topologi Jaringan

Dalam penelitian ini dibuat topology jaringan yang mensimulasikan jaringan MPLS-VPN sebagai berikut :



Gambar 3. Topologi Jaringan Simulasi

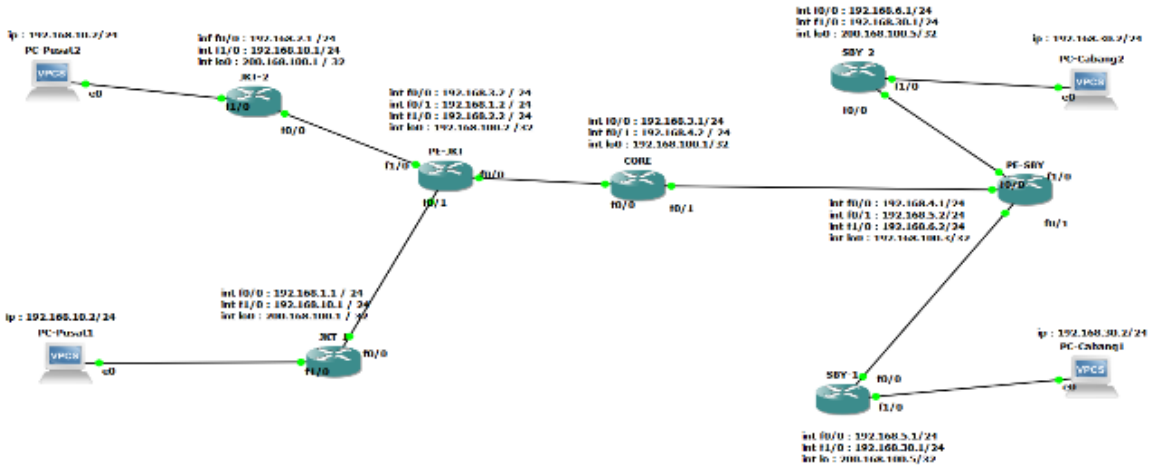
Dari topologi tersebut, ditentukan alamat network seperti pada table di bawah ini :

Tabel 4. Daftar Tabel Alamat Network

NAME	***INTERFACE***	***IP ADDRESS***
JKT-1	*Interface f0/0*	192.168.1.1/24
	Interface lo0	200.168.100.1/32
JKT-2	*Interface f0/0*	192.168.2.1/24
	Interface lo0	200.168.100.1/32
PE-JKT	*Interface f0/0*	192.168.3.4/24
	Interface f0/1	192.168.1.2/24
	Interface f1/0	192.168.2.3/24
	Interface lo0	192.168.100.2/32
Core	*Interface f0/0*	192.168.3.1/24
	Interface f0/1	192.168.4.2/24
	Interface lo0	192.168.100.1/32
PE-SBY	*Interface f0/0*	192.168.4.3/24
	Interface f0/1	192.168.5.2/24
	Interface f1/0	192.168.6.4/24
	Interface lo0	192.168.100.3/32
SBY-1	*Interface f0/0*	192.168.5.1/24
	Interface lo0	200.168.100.5/32
SBY-2	*Interface f0/0*	192.168.6.1/24
	Interface lo0	200.168.100.5/32

IV. RESULTS AND DISCUSSION

Dalam pengujin simulasi ditambahkan PC sehingga topologi jaringan dalam GNS3 sebagai berikut :



Gambar 4. Topologi Jaringan pada Simulasi GNS3

A. Hasil Pengukuran Delay

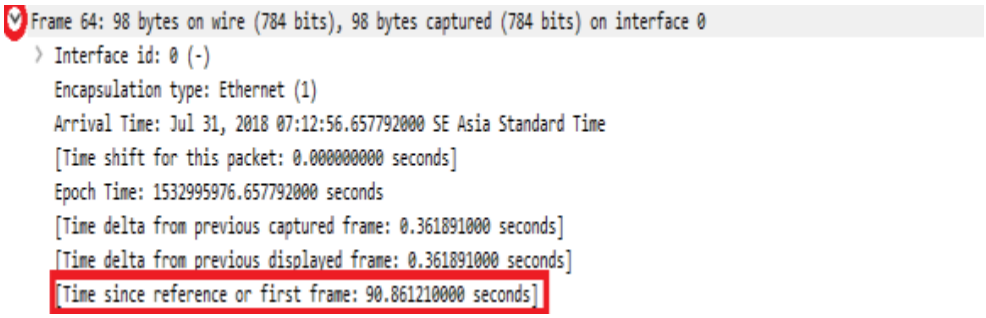
Berikut ini adalah langkah pengukuran delay menggunakan wireshark

1. Pada topologi capture link yang menghubungkan antara PC-Pusat1 dengan JKT-1 lalu pilih interface.
2. Tunggu sampai aplikasi wireshark muncul, setelah muncul di PC-Pusat1 lakukan ping ke IP PC-Cabang1, pastikan ping berhasil.
3. Pada Wireshark akan tercapture data pada saat melakukan proses ping tadi, pilih frame yang melakukan ping request dan reply, disini penulis memilih frame 63 dan frame 64
4. Klik frame63 lalu lihat kolom penjelasan frame tersebut yang berada di bawah, lalu klik tanda panah kearah kanan pada pilihan pertama lalu cari “time since reference or first frame” dimana itu merupakan waktu paket yg dikirimkan

```
Frame 63: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
  > Interface id: 0 (-)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 31, 2018 07:12:56.295901000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1532995976.295901000 seconds
    [Time delta from previous captured frame: 0.736806000 seconds]
    [Time delta from previous displayed frame: 0.736806000 seconds]
    [Time since reference or first frame: 90.786740000 seconds]
```

Gambar 5. Hasil capture waktu yang dikirimkan pada frame 63

5. Lakukan hal yang sama pada frame 64 sehingga bisa menemukan waktu yang diterima paket.



Gambar 6. Hasil capture waktu yang dikirimkan pada frame 64

Dari hasil capture tersebut dapat dihitung delay sebagai berikut :
Delay = waktu penerimaan paket - waltu pengiriman paket
= 90,861210000 - 90,786740000 = 0,07447 second = 74,47 ms
Dengan cara yang sama diperoleh pengukuran data delay seperti pada table di bawah ini.

Tabel 5. Pengukuran Delay

Pengujian	Nilai Delay (ms)
P-1	93,37
P-2	74,47
P-3	94,14
P-4	84,06
P-5	76,51
Rata – rata	84,51

B. Hasil Pengukuran Troughput

Pengukuran Troughput dengan wireshark dilakukan berdasarkan langkah-langkah berikut :

1. Pada topologi capture link yang menghubungkan antara PC-Pusat1 dengan JKT-1 lalu pilih interface.
2. Tunggu sampai wireshark berjalan dan muncul, lalu selanjutnya pilih statistics lalu pilih capture file properties, maka akan muncul kotak dialog baru, scroll down ke pilihan statistics, lihat Bytes yang merupakan jumlah data yang dikirimkan dan Time Span yang merupakan waktu pengiriman data.

Berikut ini adalah capture hasil pengukuran :

Measurement	Captured	Displayed
Packets	15	15 (100.0%)
Time span, s	23.810	23.810
Average pps	0.6	0.6
Average packet size, B	85.5	85.5
Bytes	1284	1284 (100.0%)
Average bytes/s	53	53
Average bits/s	431	431

Gambar 7. Capture Pengukuran Troughput

Dari hasil diatas didapat waktu pengiriman data 23,810 s dan jumlah data yang dikirimkan 1284 bytes maka nilai throughput nya adalah :

Troughput = Jumlah Data yang dikirimkan / Waktu Pengiriman
= 1284/23,810
= 53,92 Byte/Second

Dengan cara yang sama, dilakukan 5 sample pengukuran diperoleh hasil troughput seperti pada table dibawah ini :

Table 6. Pengukuran Troughput

Pengujian	Nilai Throughput (B/s)
P-1	67,13
P-2	70,52
P-3	69,03
P-4	53,92
P-5	78,69
Rata – rata	67,858

V. Conclusion

Setelah mendapatkan hasil dari pengujian yang dilakukan, kemudian dilakukan analisa terhadap data-data hasil pengujian tersebut. Analisa dari pengujian adalah sebagai berikut:

a. Berdasarkan parameter standar dari Thippon rata-rata delay yang diukur dari lima kali pengukuran sebesar 84,51 ms menunjukan nilai yang sangat bagus karena delay kurang dari 150 ms.
b. Untuk pengukuran troughput, dari lima kali pengukuran rata-rata nilai troughput bernilai 67,585 B/s . berdasarkan standar Thippon troughput tersebut dapat dikategorikan bagus.
c. Simulasi GNS3 dapat mendekati kondisi yang riil karena GNS3 sendiri bersifat emulator dan dapat diukur langsung dengan wireshark.

REFERENCES

[1] V. Kher, A. Arman and D. S. Saini, "Hybrid evolutionary MPLS Tunneling Algorithm based on high priority bits," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Noida, 2015, pp. 495-499, doi: 10.1109/ABLAZE.2015.7155046..

[2] Aristo, Muh. (2018). Cisco Kung Fu Jurus – Jurus Routing. Jakarta : Jasakom.

[3] Sofana, Iwan. (2016). Cisco CCNA-CCNP Routing dan Switching. Jakarta : Informatika.

[4] Cisco Indonesia, Border Gateway Protocol, Dokumen Teknis, Jakarta, Indonesia, 2012.

[5] https://www.cisco.com/c/en/us/td/docs/ios- xml/ios/qos_dfsrv/configuration/15-mt/qos- dfsrv-15-mt-book/qos-dfsrv.html.Cisco. (2014). Cisco Configuration Guide Book. [Online].

[6] Cisco. MPLS Traffic Engineering: Diffserv Configuration Guide. Dokumen Teknis, 12.4, San Jose, California, 2017.

[7] Kasmar. Differentiated Service. Dikta, Teknik Elektro dan Informatika Institut Teknologi Bandung, Bandung : 2012.

[8] GNS3, GNS3 Configuration Guide for Windows, 2012.

[9] https://www.wireshark.org/download/docs/user- guide.pdf Wireshark. (2017). Wireshark Guide. [Online].