

ANALISA PERFORMANSI TRAFIK MULTIMEDIA PADA PEMODELAN JARINGAN VPN MENGGUNAKAN METODE CLSA

Aldi Kurniawan Batubara*, Linna Oktaviana Sari**

*Teknik Elektro Universitas Riau **Jurusan Teknik Elektro Universitas Riau
Kampus Binawidya Km 12,5 Simpang Baru Panam, Pekanbaru, Riau
Jurusan Teknik Elektro Universitas Riau
Email: aldi.m.kurniawan@student.unri.ac.id

ABSTRACT

Network modeling is a way that must be learned by anyone who wants to build a network, either from the type of topology, or software that will be used. In designing a computer network based on Virtual Private Network (VPN), a networker's must have techniques or methods that are network management, so that the network can be made according to need. Network management recommended by Cisco is the Cisco Lifecycle Service Approach (CLSA) method, which manages the network until the redesign stages without changing the direction of the project's objectives. The purpose of making VPN network modeling is to see the effect of topology differences, multimedia traffic and the number of users. The design uses GNS3 v2.0.3 and VirtualBox software, where GNS3 allows complex network simulations, because it uses the original operating system from a network device such as cisco so that the computer can function like a router or even a switch. In designing this network the measuring value to be in use is throughput, delay, packet loss and jitter. Scenario testing using star topology, then do 3 multimedia traffic conditions and use the condition 1 client and 2 client. From star topology test with 3 multimedia traffic, the average delay obtained at 1 client is 34,53 ms and at 2 client equal to 57,76 ms, the average jitter obtained at 1 client is 75,2 ms and at 2 client of 114.5 ms, where the delay result <150 ms (millisecond) is categorized good according to ITU-T G.107 10 06/2015. While the average throughput obtained at 1 client of 0.150 Mb/s and at 2 clients of 0.283 Mb/s, the results obtained are categorized fairly well according to ITU-T X.135 08/97 with a good categorization of 0.628 Mb/s. For packet loss obtained at 0%, where the packet loss < 1% is categorized good according to ITU-T G.1010 11/2001.

Keyword : VPN, QoS, CLSA, GNS3 v2.0.3, VirtualBox

1. Pendahuluan

Teknologi informasi khususnya jaringan komputer menjadi alternatif yang efektif dalam meningkatnya kebutuhan masyarakat akan informasi. Dalam melakukan komunikasi dan pengelolaan informasi antara server dan client dilokasi-lokasi yang terpisah, dibutuhkan suatu jaringan internet, sehingga jaringan yang berbeda tadi terhubung dalam satu sistem jaringan komputer.

Jumlah pengguna internet di Indonesia meningkat dari tahun ke tahun. Berdasarkan data APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), data pengguna internet pada tahun 2014 mencapai 88,1 juta jiwa. APJII memproyeksikan penggunaan internet pada tahun 2015 mencapai 139 juta jiwa.

Kinerja jaringan telekomunikasi dalam proses pengiriman data sering menjadi

masalah, sehingga mempengaruhi kualitas layanan yang diberikan. Dalam transfer data diperlukan proses yang cepat dan akurat untuk meningkatkan kualitas layanan *Quality of Service (QoS)*. Semakin banyak pengguna yang mengakses data, maka kualitas akan semakin menurun karena prinsipnya adalah *sharing bandwidth*.

Penggunaan internet pada saat ini sangat rentan dari pengaruh orang luar yang secara ilegal mengakses data pribadi, sehingga diperlukannya adanya pemodelan jaringan yang bersifat aman. *Virtual Private Network (VPN)* merupakan suatu cara untuk membuat sebuah jaringan yang bersifat *private* dan aman untuk mengakses jaringan lokal dengan menggunakan sarana jaringan publik (internet). Dengan menggunakan jaringan publik ini, maka user dapat mengakses fitur-fitur yang ada

di dalam jaringan lokalnya. Didalam merancang suatu jaringan komputer yang berbasis *Virtual Private Network* (VPN), seorang *networker*'s harus memiliki teknik atau metode yang bersifat memanajemen jaringan, agar jaringan yang dirancang dapat berjalan dengan lancar sesuai kebutuhan. Salah satu manajemen jaringan yang di rekomendasikan dari cisco ialah metode *Cisco Lifecycle Service Approach* (CLSA).

Hasil telusuran penelitian terdahulu yang berkaitan mengenai *Virtual Private Network* dan *Quality of Service* ini sudah banyak dilakukan dan dikembangkan sebelumnya. Penelitian pada skripsi Muhammad Iswan tahun 2010 mengenai Implementasi *Virtual Private Network* (VPN) Remote Access dengan Linux OpenSwan (Muhammad Iswan, 2010). Pada tahun yang sama, Rosyidina Safitri melakukan implementasi dan analisa perbandingan QoS pada jaringan VPN berbasis MPLS menggunakan Routing Protokol RIPv2, EIGRP dan OSPF terhadap Tunneling IPsec untuk layanan IPBased Video Conference (Rosyidina Safitri, 2010).

Pada tahun 2012, Winky Febri melakukan perancangan jaringan dengan menggunakan IPsec VPN pada PT. Great Heart Media Indonesia (Winky Febri, 2012). Pada tahun 2013, Pham Ngoc Thanh melakukan penelitian dengan judul "*Implementation of Open Two-Factor Authentication Service Applied to Virtual Private Network*" (Pham Ngoc Thanh, 2013). Pada tahun yang sama, Daiki Imahama melakukan penelitian dengan judul "*A Reroute Method Using Multiple Routing Configurations for Fast IP Network Recovery*" (Daiki Imahama, 2013).

Pada tahun 2014, Ade Nurhayati melakukan simulasi layanan *Virtual Private Network* Internet Protocol (VPN IP) menggunakan simulator GNS3 0.8.6 (Ade Nurhayati, 2014). Pada tahun yang sama, Alex Yuasta melakukan analisis performansi Remote Access VPN berbasis IPsec dan SSL pada jaringan IPv6 (Alex Yuasta, 2014).

Pada tahun 2015, Jose Roberto melakukan penelitian dengan judul "*Analysis of the security IPv6 and Comparative study between routing protocols oriented to IPv6*"

(Jose Roberto, 2015). Pada tahun 2016, Prihatin Oktivasari melakukan analisa *Virtual Private Network* menggunakan OpenVPN dan Point to Point Tunneling Protocol (Prihatin Oktivasari, 2016). Pada tahun 2017, Baris Yamansavascular melakukan penelitian dengan judul "*Application Identification via Network Traffic Classification*" (Baris Yaman, 2017).

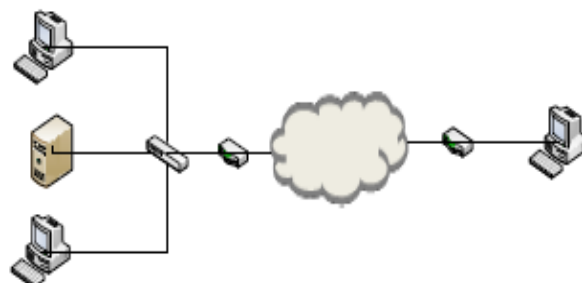
2. Landasan Teori

2.1 *Virtual Private Network* (VPN)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan seorang pegawai yang berada didalam kantor terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal. Dengan menggunakan jaringan publik ini, seorang pegawai dapat bergabung dalam jaringan local, yang mendapatkan hak dan pengaturan yang sama. (Muhammad Iswan, 2010)

2.1.1 Jenis Implementasi VPN

VPN diimplementasikan dalam dua jenis, yaitu : *remote access* dan *site to site*. *Remote access VPN* yang biasa disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN). Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software client* untuk komputer-komputer yang digunakan pegawai perusahaan tersebut. Gambar dibawah ini merupakan contoh jaringan *remote access VPN*.

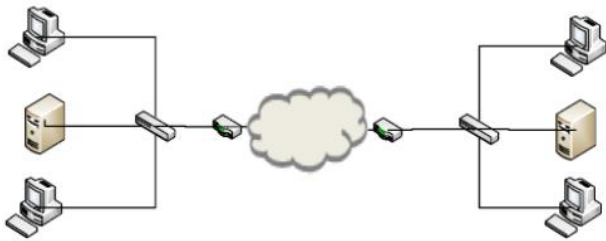


Gambar 1. Remote Access VPN

(Sumber : Alex Yuasta, 2014)

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan. VPN *site-to-site* seolah-

olah membentuk jaringan *Wide Area Network* (WAN) antar beberapa jaringan *private*. Gambar berikut menunjukkan bentuk jaringan *site-to-site* VPN.



Gambar 2. *Site-to-site* VPN
(Sumber: Alex Yuasta, 2014)

2.2 Topologi Jaringan

Topologi jaringan dalam telekomunikasi adalah suatu cara untuk menghubungkan perangkat telekomunikasi yang satu dengan yang lainnya sehingga membentuk jaringan. Ada beberapa jenis topologi Jaringan di antaranya:

- Topologi Bus adalah topologi jaringan dengan membentangkan kabel memanjang dengan kedua ujungnya ditutup dimana sepanjang kabel terdapat *node-node*.
- Topologi Star adalah topologi jaringan yang menyerupai bentuk bintang dengan *node* ditengah sebuah alat *concentrator* (*hub*, *switch*) sebagai pusat dihubungkan ke setiap *station* (komputer).
- Topologi Ring merupakan pemetaan jaringan komputer yang bentuknya seperti cincin yaitu bulatan melingkar berbentuk rangkaian titik yang masing-masing terhubung ke dua titik lainnya dimana berperan dalam menghubungkan semua komputer.
- Topologi Mesh adalah gambaran hubungan langsung antara perangkat satu dengan perangkat lainnya dimana dibangun dengan memasang link diantara *station-station*.

2.3 Graphical Network Simulator 3

GNS3 adalah software simulasi jaringan komputer berbasis GUI yang mirip dengan Cisco Packet Tracer. Namun pada GNS3 memungkinkan simulasi jaringan yang kompleks, karena menggunakan operating

system asli dari perangkat jaringan seperti cisco dan juniper. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi router langsung daripada di Cisco Packet Tracer.

GNS3 merupakan alat pelengkap yang sangat baik untuk laboratorium nyata bagi network engineer, karena GNS3 mensupport beberapa jenis aplikasi virtual lainnya seperti Pemu, Qemu, Virtual Box dan dapat mensupport virtual yang lainnya. Router virtual yang terdapat di GNS3 juga dapat dikoneksikan ke hardware yang sebenarnya.

Prinsip kerja dari GNS3 adalah mengemulasi Cisco IOS pada komputer, sehingga PC dapat berfungsi layaknya sebuah atau beberapa router bahkan switch, dengan cara mengaktifkan fungsi dari Ethernet Switch Card. (Jason C, 2015)

Berikut ini merupakan bentuk dari tampilan dari *Software* GNS3 v1.4.6



Gambar 3. Bentuk tampilan *Software* GNS3 v1.4.6

2.4 Parameter *Quality of Service*

Untuk Kerja dari suatu jaringan dapat diamati dari parameternya. Beberapa parameter utama dari sebuah jaringan akan dijelaskan sebagai berikut.

2.4.1 Troughput

Throughput adalah *bandwidth* sebenarnya (aktual) yang di ukur dengan satuan waktu tertentu yang digunakan untuk melakukan *transfer* data dengan ukuran tertentu. Waktu *download* terbaik adalah ukuran *file* di bagi dengan *bandwidth*. Sedangkan waktu aktual atau sebenarnya adalah ukuran *file* di bagi dengan *throughput*. Untuk menghitung *throughput* dapat dihitung dengan persamaan 1. (Vilho Raisenen, 2003)

$$\text{Troughput} = \frac{\text{Jumlah data yang dikirim}}{\text{Total waktu pengiriman}} (\text{bps}) \dots\dots(1)$$

2.4.2 Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal hingga ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Untuk menghitung *delay* rata -rata dapat dilihat pada persamaan 2. (Vilho Raisenen, 2003)

$$\text{Delay rata - rata} = \frac{\text{Total delay}}{\text{Total paket yang diterima}} \dots\dots(2)$$

Berdasarkan versi *ITU-T (International Telecommunication Union - Telecommunication)* standarisasi nilai *delay / latency* sebagai berikut.

Tabel 1. Performansi kinerja jaringan berdasarkan *delay*

Kategori Latency	Besar Delay
Baik	< 150 ms
Cukup	150 s/d 400 ms
Buruk	> 400ms

(Sumber : ITU-T G.107 10 06/2015)

2.4.3 Jitter

Jitter diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan jitter. *Jitter* lazimnya disebut variasi delay, berhubungan erat dengan latency, yang menunjukkan banyaknya variasi delay pada transmisi data di jaringan. Dilihat dari persamaan 2.3. (Vilho Raisenen, 2003)

$$\text{Jitter} = \frac{\text{Total variasi delay}}{\text{Total paket yang diterima}} \dots\dots(3)$$

2.4.4 Packet Loss

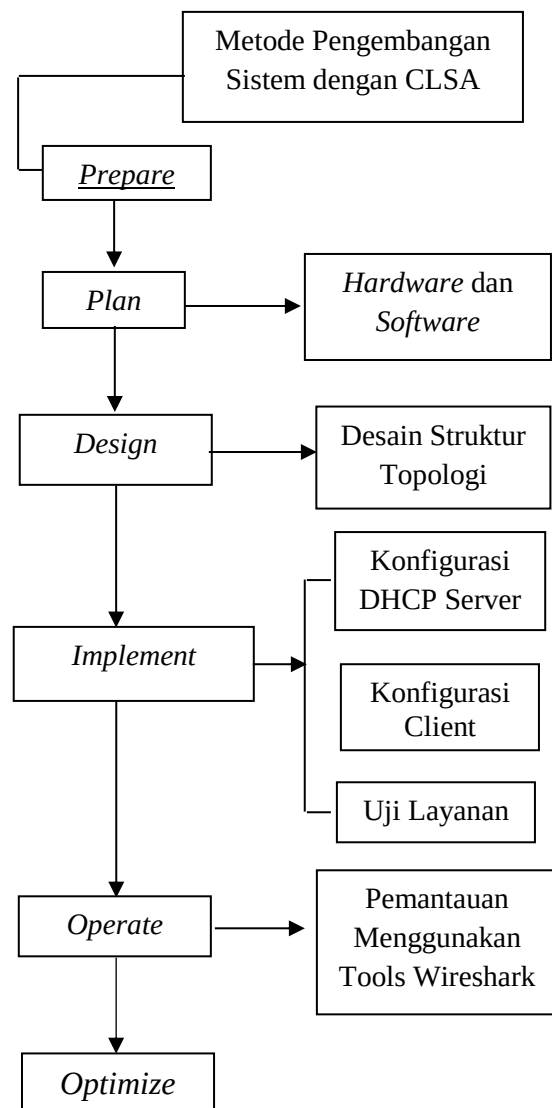
Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi karena *collision* dan *congestion* pada jaringan. Untuk menghitung *packet loss* dapat dihitung dengan persamaan 2.4. (Vilho Raisenen, 2003)

$$\text{Packet Loss} = \frac{\text{packet data yang dikirim} - \text{paket data yang diterima}}{\text{Paket data yang dikirim}} \dots\dots(4)$$

3. Metodologi

3.1 Metode Penelitian

Metode yang digunakan dalam pengembangan ini adalah metode *Cisco Lifecycle Service Approach (CSLA)*, pada setiap phase dalam sebuah lifecycle pengembangan jaringan, dibutuhkan pada setiap bagian dengan kesesuaian bisnis dan kebutuhan teknis dari perusahaan tersebut. (Richard Froom, 2010)



Gambar 4. Metode penelitian dengan menggunakan Metode Pengembangan *Cisco Lifecycle Service Approach*.

3.2 Alat dan Bahan

Berbagai elemen atau komponen yang mencakup pembuatan penelitian ini :

1. Spesifikasi Software

Ada beberapa *software* yang perlu disiapkan pada perancangan jaringan VPN berikut ini :

Tabel 2. Spesifikasi Software

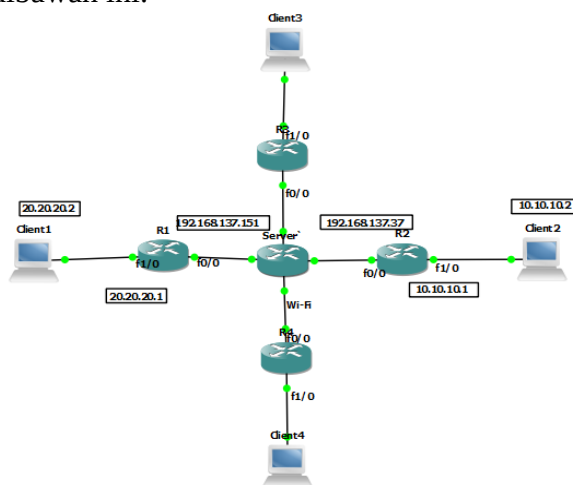
No	Software	Keterangan
1	GNS3 v2.0.3	Simulasi Perancangan
2	Virtual Box	Sistem operasi untuk VPN <i>Client</i>
3	Wireshark	Monitoring Kinerja

2. Spesifikasi Hardware

- Komputer VPN server dengan spesifikasi Windows 10, AMD Quad-Core 2.0Ghz, Harddisk 500 GB, DVD-Super Multi DL Drive, RAM 4 GB dan monitor 14.0" HD.
- Dua PC menggunakan Software Virtual Box dengan spesifikasi RAM 1024 dan 2048, Windows 7.

3.3 Desain Topologi Jaringan

Desain topologi pada pemodelan jaringan VPN akan dilakukan pengujian diambil berdasarkan topologi yang sudah ditetapkan yaitu topologi *star* dapat dilihat pada gambar dibawah ini.



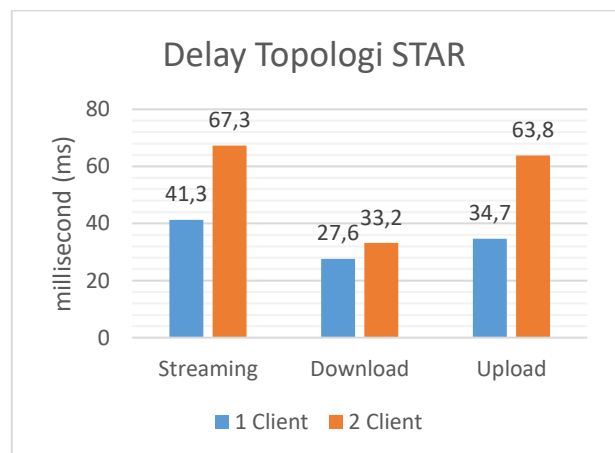
Gambar 5. Perancangan Jaringan Topologi *Star* menggunakan GNS3
Keterangan IP :

Tabel 3. Keterangan IP Jaringan VPN

No	Elemen	Transmisi	IP
1	R1	f0/0 dan f1/0	DHCP 192.168.1.1
2	R2	f0/0 dan f1/0	192.16.1.2 10.1.1.1
3	R5	f0/0 dan f1/0	DHCP 172.16.1.1
4	R6	f0/0 dan f1/0	172.16.1.2 20.20.20.1
5	Windows 7	NIC	10.10.10.2
6	Windows 7	NIC	20.20.20.2
7	Server	NIC	192.168.137.1

4. Hasil dan Pembahasan

4.1. Delay

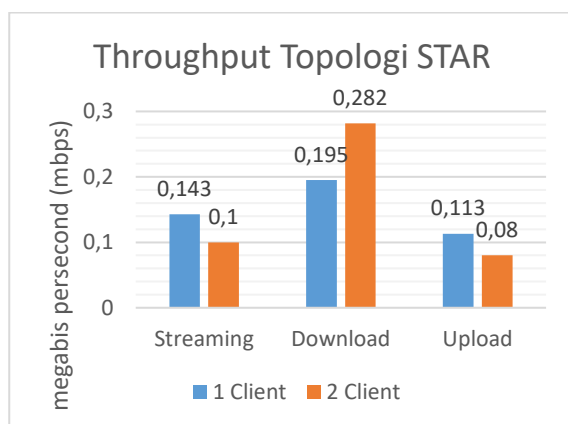


Gambar 6. Grafik Perbandingan Delay Topologi *Star* pada 1 Client dan 2 Client

Pada gambar 6. terlihat perbedaan *delay* saat melakukan proses *streaming*, *download* dan juga *upload* pada topologi *star* yang menggunakan 1 *client* dan 2 *client*. Pada proses *streaming* dengan 1 *client* *delay* yang dihasilkan sebesar 41,3 ms sedangkan 2 *client* memiliki *delay* 67,3 ms. Pada saat melakukan proses *download* dengan 1 *client* maupun 2 *client* memiliki besar *delay* yang tidak terlalu

signifikan yaitu sebesar 27,6 ms dan 33,2 ms sedangkan pada proses *upload* dengan 1 *client* memiliki *delay* 34,7 ms dan 63,8 ms pada 2 *client*. Hal ini membuat topologi *star* dengan 1 *client* maupun 2 *client* memiliki *delay* yang berbeda dikarenakan seberapa banyak *client* yang mengakses jaringan server tersebut. Sehingga semakin banyak jumlah *client* yang mengakses jaringan tersebut maka *delay* akan semakin naik. Hal ini disebabkan karena server yang terbebani oleh banyaknya pengguna serta spesifikasi perangkat yang jauh lebih tinggi dan kapasitas RAM yang mendukung.

4.2. Throughput

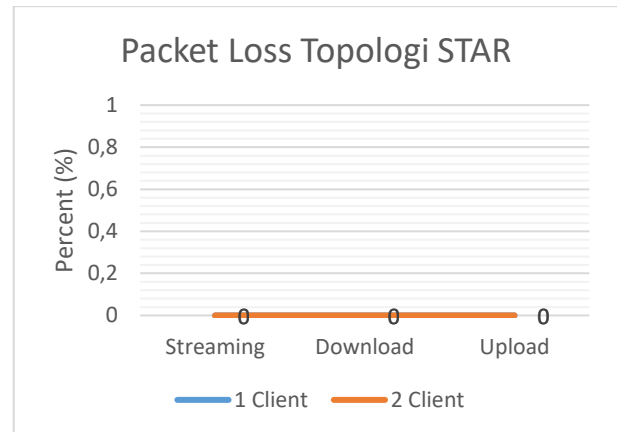


Gambar 7. Grafik Perbandingan *Throughput* Topologi *Star* pada 1 *Client* dan 2 *Client*

Pada gambar 7. terlihat perbedaan nilai *throughput* saat melakukan proses *streaming*, *download* dan juga *upload* pada topologi *star* yang menggunakan 1 *client* dan 2 *client*. Pada proses *streaming* dengan 1 *client* memiliki *throughput* 0,143 *Mbits/s*, sebesar 0,195 *Mbits/s* saat *download* dan sebesar 0,113 *Mbits/s* saat *upload*. Sedangkan dengan 2 *client* memiliki *throughput* 0,100 *Mbits/s* saat *streaming*, sebesar 0,282 *Mbits/s* saat *download* dan sebesar 0,08 *Mbits/s* saat *upload*. Hal ini membuat topologi *star* dengan 1 *client* maupun 2 *client* memiliki *throughput* yang berbeda dikarenakan pada saat *streaming* pengaruh lamanya pengambilan *packet* serta kualitas video yang berbeda antara 240pixel dengan 480pixel, sedangkan saat *download* dan *upload* dipengaruhi oleh ukuran *size*. Sehingga semakin besar kualitas video yang diakses, semakin kecil *throughput* yang dihasilkan, tetapi hal ini juga dipengaruhi oleh kecepatan

internet access yang diperoleh disetiap *client* yang dibentuk serta pengaruh spesifikasi perangkat yang jauh lebih tinggi dan kapasitas RAM yang mendukung.

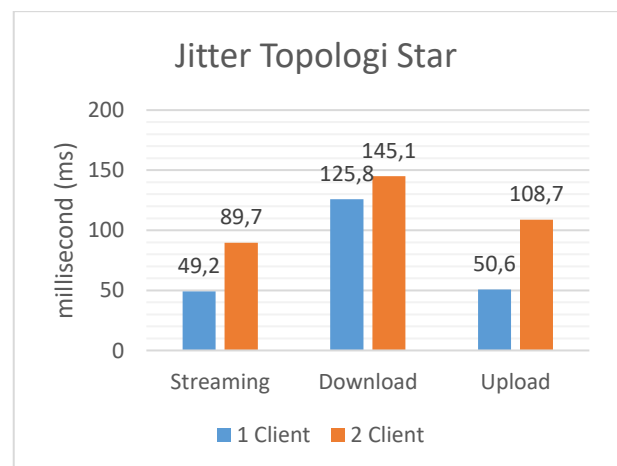
4.3. Packet Loss



Gambar 8 Grafik Perbandingan *Packet Loss* Topologi *Star* pada 1 *Client* dan 2 *Client*

Pada gambar 8. terlihat bahwa nilai perbedaan *packet loss* antara topologi *star* yang menggunakan 1 *client* dan 2 *client*. Topologi *star* dengan 1 *client* memiliki *packet loss* 0 % pada saat melakukan proses *streaming*, *download*, *upload* dan pada topologi *star* dengan 2 *client* juga memiliki *packet loss* sebesar 0% saat melakukan proses *streaming*, *download* dan *upload*. Hal ini membuat topologi *star* dengan 1 *client* maupun 2 *client* memiliki nilai *packet loss* yang baik pada melakukan proses *streaming*, *download* dan *upload*.

4.4. Jitter



Gambar 9. Grafik Perbandingan *Jitter* Topologi *Star* pada 1 *Client* dan 2 *Client*

Pada gambar 9. terlihat perbedaan nilai *jitter* saat melakukan proses *streaming*, *download* dan juga *upload* pada topologi *star* yang menggunakan 1 *client* dan 2 *client*. Pada proses *streaming* dengan 1 *client* memiliki *jitter* 49,2 ms, sebesar 125,8 ms saat *download* dan sebesar 50,6 ms saat *upload*. Sedangkan topologi *star* dengan 2 *client* memiliki *jitter* sebesar 89,7 ms saat *streaming*, sebesar 145,1 ms saat *download* dan sebesar 108,7 ms saat *upload*. Hal ini membuat nilai *jitter* dengan 1 *client* saat lebih baik dibanding 2 *client*. Sehingga pengaruh lamanya pengambilan *packet* sangat berpengaruh dengan nilai yang dihasilkan untuk *jitter*, dapat dikatakan semakin besar jumlah *packet* semakin besar pula *jitter* yang dihasilkan.

5. Kesimpulan

Setelah dilakukan proses perancangan, pengujian serta analisa dan juga membandingkannya dengan teori-teori penunjang, maka dapat disimpulkan bahwa:

1. Penambahan jumlah *client* atau pengguna dapat menyebabkan terjadinya penurunan QoS pada semua topologi yang diujikan. Hal ini dikarenakan *server* yang terbebani oleh banyaknya *client* yang mengakses jaringan tersebut.
2. Pada pengujian topologi *star* dengan 3 trafik *multimedia*, rata-rata *delay* yang didapat pada 1 *client* sebesar 34,53 ms dan pada 2 *client* sebesar 57,76 ms. Rata-rata *jitter* yang didapat pada 1 *client* sebesar 75,2 ms dan pada 2 *client* sebesar 114,5 ms. Sedangkan rata-rata *throughput* yang didapat pada 1 *client* sebesar 0,150 Mbits/sec dan pada 2 *client* sebesar 0,283 Mbits/sec, untuk *packet loss* yang didapat sebesar 0%. Penurunan QoS ini disebabkan oleh perbedaan bentuk trafik yang diujikan, lamanya waktu pengambilan *packet* serta *server* yang terbebani oleh beberapa pengguna, sehingga semakin banyak jumlah pengguna semakin turun QoS yang didapat.

Daftar Pustaka

- APJII, 2014. Profil Penggunaan Internet Indonesia Tahun 2014. Pusat Kajian Komunikasi Universitas Indonesia.
- Ade Nurhayati, Qonithatul Azizah. 2014. "Simulasi Layanan Virtual Private Network Internet Protocol (VPN IP) Menggunakan Simulator GNS3 0.8.6", Akademi Telkom Jakarta, Jakarta.
- Baris Yamansavascilar, M. Amac Guvenson, A. Gokhan Yavuz, M. E.Karsligil. 2017. "Application Identification via Network Traffic Classification". Department of Computer Engineering, Yildiz Technical University. Istanbul-Turkey.
- Cisco Systems, 2003. "Internetworking Technologies Handbook". Fourth Edition. Cisco Press
- Daiki imahama, Yukinobu Fukushima, Tokumi Yokohira. 2013. "A Reroute Method Using Multiple Routing Configurations for Fast IP Network Recovery". The Graduate School of Natural Science and Technology, Okayama University. Japan.
- Muhammad Iswan. 2010. "Implementasi Virtual Private Network (VPN) Remote Access dengan Linux OpenSwan". Fakultas Sains dan Teknologi Program Studi Teknik Informatika, Univesitas Islam Negeri Syarif Hidayatullah. Jakarta.
- Jason C. Neumann. 2015. "The Book of GNS3". Build Virtual Network Labs Using Cisco, Juniper, and More. San Francisco.
- Jose Roberto Patino Sanchez. 2015. "Analysis of the security IPv6 and Comparative study between routing protocols oriented to IPv6". Faculted de Ingenieria en Electricidad y Computacion. Guayaquil-Ecuador.
- Oracle VM VirtualBox. 2017. "User Manual". OracleCorporation.<http://www.virtualbox.org>

- Pham Ngoc Thanh, Keeheon Kim. 2013. “*Implementation of Open Two-Factor Authentication Service applied to Virtual Private Network*”. Dept. of Computer Science. Konkuk University, Seoul, South Korea.
- Prihatin Oktivasari, Andri Budhi Utomo. 2016. “*Analisa Virtual Private Network Menggunakan OpenVPN dan Point to Point Tunneling Protocol*”. Politeknik Negeri Jakarta. Jakar.
- Richard Froom, Balaji Sivasubramanian, Erum Frahim. 2010. “*Implementing Cisco IP Switched Networks (Switch). Foundation Learning Guide*. Cisco Press. United States of America.
- Rosyidina Safitri. 2010. “*Implementasi dan Analisa Perbandingan QoS pada Jaringan VPN Berbasis MPLS menggunakan Routing Protocol RIPv2, EIGRP dan OSPF terhadap Tunneling IPsec untuk Layanan IP-Based Video Conference*”. Universitas Indonesia. Jakarta.
- Standar Cisco Confidential. “*An Introduction to The Cisco Lifecycle Service Approach*”. <https://www.cisco.com>. Diakses pada tanggal 27 Oktober 2017.
- Standar Delay ITU-T G.107 10 06/2015. <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12505&lang=en>. Diakses pada tanggal 25 Oktober 2017.
- Vilho, Raisanen. 2003. “*Implementing Service Quality in IP Networks*”. Nokia Networks OY. Finland.