Jurnal ICT Vol V, No. 9, Nov 2014 , 24-30

AKADEMI TELKOM SANDHY PUTRA JAKARTA

SIMULASI LAYANAN VIRTUAL PRIVATE NETWORK INTERNET PROTOCOL (VPN IP) MENGGUNAKAN SIMULATOR GNS3 0.8.6

Jurusan Teknik Telekomunikasi
[1)]Ade Nurhayati, [2)] Qonithatul Azizah
Akademi Teknik Telekomunikasi Jakarta
[1)]Ade_nurhayati13@yahoo.com [2)]Qonitathulazizah@gmail.com

Abstrak

Virtual Private Network Internet Protocol (VPN IP) merupakanjaringan *private* secara virtual diatas jaringan *public* (umum) seperti internet dan merupakan jaringan *point to point*. VPN berkembang dikarenakan adanya perkembangan yang pesat pada perusahaan-perusahaan besar yang ingin tetap memperluas jaringan bisnisnya.Pada penelitian ini akan dibahas simulasi jaringan VPN IP dalam mengirimkan paket data kepada *user* dari *server*. Pembuatan VPN IP ini memerlukan *routingprotocol* yaitu *PointtoPointProtocol* (PPTP), Layer 2 *Tunneling Protocol* (L2TP), atau IP Sec.

Kemudian menggunakan algoritma kripthography tertentu seperti DES, 3DES, atau AES. Dan hasil yang didapatkan dari simulasi ini dapat diimplementasikan dengan baik. yang biasa digunakan dalam suatu institusi perusahaan yang ingin mengembangkan bisnisnya khususnya melalui jalur komunikasi.

Kata Kunci : VPN IP, 3DES, DES, AES, PROTOCOL VPN IP

Abstrack

Virtual Private Network Internet Protocol (VPN IP) is a virtual private network over a public network (general) such as the Internet and is a point-to-point network. VPN growing due to rapid development in large companies who want to keep expanding its business network. This Final Project will be discussed in a simulation of an IP VPN network to send data packets to the user from the server. This requires making a VPN IP routing protocols, namely Point to Point Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), or IP Sec.

Then, using algorithms such as DES kripthography, 3DES, or AES. And the results obtained from these simulations can be implemented properly. commonly used in institutions that want to develop their business enterprise particularly through the communication line.

Key Words : VPN IP, 3DES, DES, AES, PROTOCOL VPN IP

1. PENDAHULUAN

1.1. Latar Belakang

Kebutuhan masyarakat untuk berkomunikasi dengan mudah secara efisien menggunakan internet semakin bertambah dari waktu ke waktu, kebutuhan ini berkembang seiring dengan mobilitas masyarakat yang cukup tinggi bisa dikarenakan oleh pekerjaan atau gaya hidup dan tidak mampu dipenuhi dengan perangkat telekomunikasi yang telah ada sebelumnya yaitu dengan telepon rumah (fixed wireline phone).

Perkembangan telekomunikasi di dunia sangatlah pesat saat ini, jika kita melihat dari sisi teknologi, dan jenis topologi pasti semakin berkembang. Dewasa ini, kebutuhan user akan informasi semakin besar, kebutuhan akan layanan, kecepatan, dan bandwidth. Hal tersebut menghasilkan teknologi-teknologi jaringan yang lebih baik yang lebih menjanjikan. Tidak hanya teknologi dan pelayanan yang berkembang, protocol-protocol jaringan semakin berkembang mengikuti teknologi yang semakin baik.

User pada saat ini dapat berkomunikasi tidak hanya menggunakan telepon yang masih berbasis sircuit switch. Sekarang user dapat memperoleh informasi dengan cara yang lebih efisien dengan teknologi berbasis packet switch yang berstandarkan alamat IP (Internet Protocol).

Internet merupakan sebuah jaringan global dan terbuka, dimana setiap pengguna dapat saling berkomunikasi dan bertukar informasi. Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan biaya dan privasinya menjadi faktor utama.

Untuk mengatasi masalah bandwidth dan privasi dalam komunikasi data pada jaringan umum (public network/internet) maka lahirlah Virtual Private Network (VPN). VPN merupakan singkatan dari Virtual Private Network yang artinya membuat jaringan private secara virtual diatas jaringan public(umum) seperti internet. VPN berkembang dikarenakan adanya perkembangan yang pesat pada perusahaan-perusahaan besar yang ingin tetap memperluas jaringan bisnisnya. Didalam VPN terdapat perpaduan teknologi tunneling dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan.

1.2 Tujuan

Maksud dan tujuan dalam penelitian ini adalah Membuat software simulasi pengiriman paket data VPN IP menggunakan GNS3 Versi 0.8.6 sebagai tutorial.

1.3 Metodologi Penelitian

1. StudiLiteratur

Metode ini dilakukan dengan melakukan studi literatur di Perpustakaan kampus atau di Perpustakaan lain yang berhubungan dengan permasalahan yang akan dibahas, dan membaca buku referensi serta mencari data di situs internet yang dapat mendukung perealisasian penelitian ini.

2. RisetdanAplikasi

Melakukan penelitian tentang proses yang dilakukan dengan dibimbing oleh staf yang sudah ahli di bidangnya.

2. DASAR TEORI

2.1. VPN IP

Virtual Private Network Internet Protocol atau VPN IP adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik yang mengirimkan layanan Internet Protocol (IP) private, yang menjadi kunci VPN IP adalah pengiriman layanan IP kepada end user.

VPN IP berbasis jaringan publik yang berjalan di platform IP sehingga pengiriman layanan lebih bersifat *connectionless*, dalam artian data terkirim begitu saja tanpa ada proses pembentukan jalur terlebih dahulu (*connectionsetup*).

VirtualPrivateNetwork menciptakan suatu WAN yang sebenarnya terpisah baik secara fisikal maupun geografis sehingga secara logika membentuk satu network tunggal, paket data yang mengalir antar site maupun dari user yang melakukan remote akses akan mengalami enkripsi dan authentikasi sehingga menjamin keamanan, integritas dan validitas data.

VPN (*VirtualPrivateNetwork*) dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara point-to-point. Data dienkapsulasi (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan koneksi point-to-point sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses deskripsi. Proses enkapsulasi data sering disebut "*tuneling*". [7]

Gambar 1. Jaringan Virtual Private Network Internet Protocol

2.2. Sistem Keamanan VPN

Sistem keamanan VPN menggunakan beberapa metode lapisan sistem keamanan, diantaranya :

1. Metode tunneling (terowongan), membuat terowongan virtual diatas jaringan publik menggunakan protocol seperti Point to Point Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE) atau IP Sec. PPTP dan L2TP adalah layer 2 tunneling protocol, keduanya melakukan pembungkusan payload pada frame Point to Point Protocol (PPP) untuk di lewatkan pada jaringan. IPSec berada di layer 3 yang menggunakan packet, yang akan melakukan pembungkusan IP header sebelum dikirim ke jaringan.
2. Metode Enkrpsi untuk Encapsulations (membungkus) paket data yang lewat didalam tunneling, data yang dilewatkan pada pembungkusan tersebut, data disini akan dirubah dengan metode algoritma kripthography tertentu seperti DES, 3DES, atau AES.
3. Metode Otentikasi User, karena banyak user yang akan mengakses biasanya digunakan beberapa metode otentikasi user seperti Remote Access Dial In User Services (RADIUS) dan Digital Certificates.
4. Integritas Data, paket data yang dilewatkan di jaringan publik perlu penjaminan integritas data / kepercayaan data apakah terjadi perubahan atau tidak. Metode VPN menggunakan HMA C-MD5 atau HMA CSHA1 untuk menjadi paket tidak dirubah pada saat pengiriman [8].

Protokol-protokol VPN IP adalah sebagai berikut [7]:

a. Layer 2 Tunneling Protocol (L2TP)
b. Point-Point Tunneling Protocol (PPTP)
c. IPsec (Internet Protocol Security)

III. Graphical Network Simulator 3 (GNS3)

3.1 Konsep GNS3

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. Dynamips adalah program inti dari GNS3

yang memungkinkan sebuah emulasi IOS Cisco berjalan. Dynamips dioperasikan diatas aplikasi GNS3 sehingga membuat suatu environtment yang lebih friendly user dengan menggunakan grafik dalam pengoperasian aplikasi tersebut.

GNS3 adalah 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.

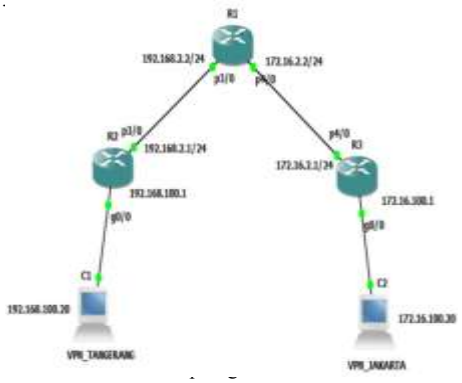
3.2 MEMBANGUN LAYANAN VPN IP MENGGUNAKAN GNS3 0.8.6

Simulasi ini bertujuan untuk melatih pada engineer muda memahami jaringan layanan VPN IP yang ada di suatu perusahaan namun tidak dapat mempelajarinya secara langsung karena keterbatasan waktu, memperoleh izin, dan lembaganya sangat terbatas.

Berikut standar Hardware dan software yang diperlukan dalam simulasi VPN IP :

1. Tiga PC dengan Processor berkapasitas Core 2 Quad (Intel Core I3 Recommended).
2. Adapter LAN dengan USB 3.0 Gigabit Ethernet yang di pasang di slot PC.
3. Kapasitas RAM minimum 4 GB (8 GB recommended)
4. Kapasitas hardisk minimum 500 GB (750 recommended)
5. Software GNS3 0.8.6

Berikut topologi jaringan VPN IP yang penulis gambarkan :



Keterangan IP :

R1	P3/0	192.168.2.2/24
	P4/0	172.16.2.2/24
R2	P3/0	192.168.2.1/24
	Gateway	192.168.100.1
R3	p4/0	172.16.2.1
	Gateway	172.16.100.1
VPN_Tangerang		192.168.100.20
VPN_Jakarta		172.16.100.20

Setelah mengintal software GNS3, kemudian mengkonfigurasi router yang akan digunakan yaitu Router Cisco 7200.

Gambar 3. Konfigurasi slot Adapter IOS IMAGE Router Cisco 7200 pada R1

Gambar 4. Konfigurasi slot Adapter IOS IMAGE Router Cisco 7200 pada R2

Gambar 5. Konfigurasi slot Adapter IOS IMAGE Router Cisco 7200 pada R3

Setelah konfigurasi slot, hubungkan setiap router sesuai topologi dan aktifkan masing-masing router.

Gambar 5. Konfigurasi Idle PC

Kemudian pilih nilai yang sesuai atau nilai yang diberi tanda bintang (*). Masing-masing router pasti akan mendapatkan nilai idle PC yang berbeda beda.

Setelah itu Penulis mengkonfigurasi setiap router dengan cara klik kanan pada roter – klik *Console*.

Setelah mengkonfigurasi semua router makan Penulis melakukan verivikasi jaringan, apakah link sudah terhubung.

Contoh : Penulis melakukan ping pada network 192.168.2.1/24 yang berada di R2 ke network 172.16.2.1/24 yang berada pada R3.

Gambar 7. Verifikasi link pada network

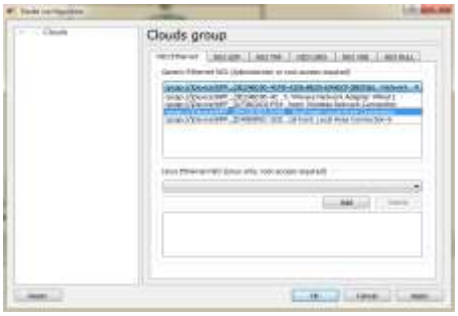
Langkah pertama yang Penulis lakukan setalah mengkonfigurasi router adalah mengkonfigurasi sistem adapter yang akan dihubungkan ke Jaringan VPN IP yang berada di GNS3, sebagai berikut :

Buatlah link PC virtual yang telah dibuat ke router yang telah di konfigurasi, sebagai berikut :

1. Klik kanan pada virtual PC pertama (VPN_Tengerang) pilih Local Area Network 6. Kemudian klik OK.

Gambar 8.Konfigurasi IP pada komputer server

Pada virtual PC kedua (C2) pilih Local Area Network, kemudian klik OK.



Gambar 9. Konfigurasi Adapter Local Area Network pada virtual komputer (C2)

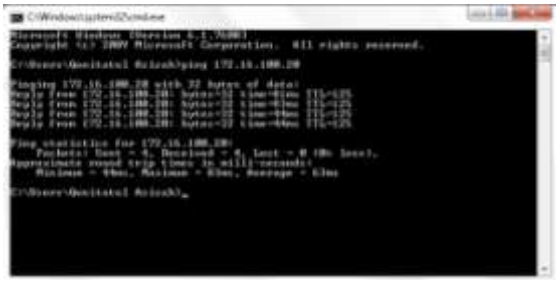
2. Penyettingan IP Local Area Network pada komputer server.
   Dengan alamat IP 172.16.100.20/24
   Gateway 172.16.100.1
   DNS 172.16.0100.1

Gambar 10. Konfigurasi Adapter Local Area Network 6 pada virtual komputer (C1)

3. Penyettingan IP Local Area Network pada komputer Client.
   Dengan alamat IP 192.168.100.20/24
   Gateway 192.168.100.1
   DNS 192.168.100.1

Gambar 11. Konfigurasi IP pada komputer client

4. Patikan bahwa IP user dengan subnet 192.168.100.20/24 terhubung dengan IP server dengan alamat IP 172.168.100.20/24.

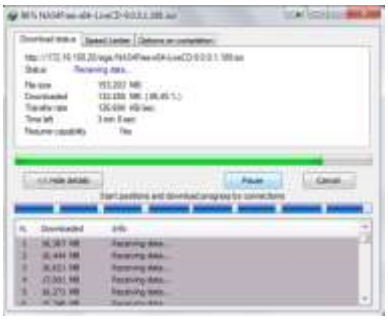


Gambar 12. Konfigurasi IP pada komputer client

5. Setelah memastikan koneksi ke server terhubung, Penulis menjalankan layanan WEB Server yang tersedia diserver 172.16.100.20/24

Gambar 13. Halaman WEB Server

6. Download file dari halaman web server menggunakan Internet Download Manager untuk mengetahui seberapa besar kapasitas bandwidth, kecepatan pengiriman (Bit Rate), serta delay yang terjadi. File yang di download pada pengujian ini adalah file ISO NAS4 x64 bit dengan size 153.203 MB.



Gambar 14. Download di PC Client

7. Penulis juga mencoba layanan video streaming pada jaringan VPN IP dengan menggunakan software VLC (Video LAN Connection). Setelah mengintegrasikan PC server dengan Client menggunakan VLC, kemudian masukkan alamat IP server dan port pada kotak dialog Jaringan/Network seperti gambar dibawah ini. Setelah itu klik Stream, maka VLC dari pihak Client akan melakukan pengambilan data (buffer) dan segera menampilkan video yang di streaming oleh server.

Gambar 15. Open Network Stream

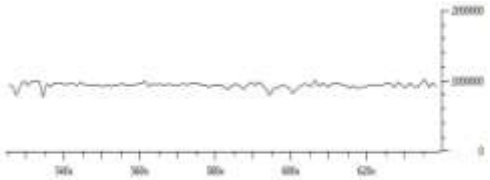
IV. ANALISA HASIL SIMULASI LAYANAN VPN IP MENGGUNAKAN SIMULATOR GNS3 0.8.6

4.1 Mengukur Parameter QOS (Quality Of Service) Pengiriman Paket Data Dengan Menggunakan Wireshark.

1. Bandwidth

Bandwidth adalah besaran yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam koneksi melalui sebuah network. Kemampuan maksimum dari suatu alat untuk menyalurkan informasi dalam satuan waktu detik (bit/sekon).

Penulis memanfaatkan layanan Wireshark untuk mengetahui besarnya Bandwidth yang dihasilkan pada pengiriman paket data antara VPN IP Tangerang (Server) dan VPN IP Jakarta (Client) pada simulasi ini. Pada simulasi ini, jenis paket data yang di download dari server adalah file ISO.



Gambar 16. Grafik Bandwidth pada subnet 192.168.100.20/24

Pada gambar 16. di atas dapat dilihat grafik bandwidth saat pengiriman paket data. Grafik bandwidth menunjukkan kestabilannya pada saat pengiriman data berlangsung, ini dikarenakan cara yang dilakukan dan media yang digunakan dalam pengiriman paket sesuai dengan standar pada simulasi sehingga pengiriman paket berjalan stabil tanpa collusion data.

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	162626	162626	100.000%	0	0.000%
Between first and last packet	1321.426 sec				
Avg. packets/sec	123.069				
Avg. packet size	895.662 bytes				
Bytes	145657976	145657976	100.000%	0	0.000%
Avg. bytes/sec	110227.856				
Avg. MBit/sec	0.882				

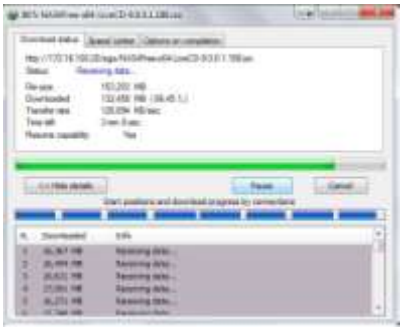
Gambar 17.Summary

Dari data perhitungan bandwidth diatas bahwa nilai Bandwidth pada perhitungan Wireshark adalah 0,882 Mbps. Beberapa faktor yang menentukan bandwidth adalah:

a. Perangkat jaringan.
b. Tipe data yang ditransfer
c. Topologi jaringan
d. Banyaknya pengguna jaringan
e. Spesifikasi komputer client/user
f. Spesifikasi komputer server
g. Dan lain-lain

2. Bit Rate

Bit Rate adalah jumlah rata –rata nilai bit yang diperlukan untuk mengirimkan data dalam satuan waktu tertentu. Pengukuran umum dari bitrate biasanya menggunakan istilah kilobyte per second (kbps) dan Megabyte per second (Mbps). Apapun unit yang tengah diukur, semakin tinggi angka bitrate, maka kualitas file semakin bagus atau semakin cepat. Bit Rate yang didapat saat pengiriman paket dari server ke client, menurut hasil capture Internet Download Manager :



Gambar 17. Capture Bit Rate di IDM

Pada gambar 17. diatas, bit rate yang dihasilkan adalah sebesar 126.694 KB/sec. Jumlah ini memang tidak cukup besar dari yang seharusnya dikarenakan faktor, yaitu :

1. Media transmisi yang digunakan adalah kabel UTP yang berkapasitas maksimal 100 Mbps.
2. Terdapat virus pada komputer client atau server, terdapat Noise Thermal pada PC, dikarenakan penggunaan PC yang berlebihan.
3. Spesifikasi perangkat PC dan media transmisi yang belum maksimal
4. Dan lain-lain.

Dimana dalam kondisi real rata-rata kecepatan pada jaringan VPN IP dapat mencapai 1,5 – 2 Mb/Sec. Dikarenakan faktor berikut :

1. Media transmisi yang digunakan pada kondisi real menggunakan fiber optik yang kecepatan maksimumnya mencapai 1 Gbps
2. Spesifikasi perangkat yang jauh lebih lebih tinggi dan mendukung, karena jaringan tersebut adalah jaringan global yang memang seharusnya menggunakan perangkat dengan spesifikasi yang tinggi.
3. Kapasitas RAM yang besar pada server
4. Dan lain-lain.

3. Delay

Delay adalah waktu yang dibutuhkan untuk mentransmisikan data sampai ke penerima. Delay yang didapat menurut hasil capture Wireshark :

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	162626	162626	100.000%	0	0.000%
Between first and last packet	1321.426 sec				
Avg. packets/sec	123.069				
Avg. packet size	895.662 bytes				
Bytes	145657976	145657976	100.000%	0	0.000%
Avg. bytes/sec	110227.856				
Avg. MBit/sec	0.882				

Gambar 18. Delay pada Subnet 192.168.100.20/24

Pada gambar 4.4 diatas diperlukan waktu untuk mengirimkan paket data sebanyak 162626 dari server ke client

$$\text{Delay} = \frac{\text{Waktu Pengiriman}}{\text{Total paket data yang diterima}}$$

$$= \frac{1321.426}{162626}$$

$$= 8.125 \times 10^{3} = 8{,}125 \text{ milisecon}$$

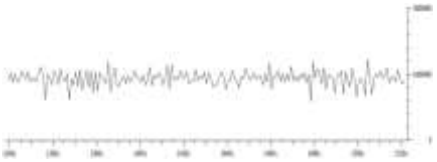
adalah 1321.426 sec. Sehingga dapat dihitung besar delay perpaket yang terjadi dengan persamaan berikut :

Parameter delay didefinisikan pada IETF RFC 3393 (November, 2002) IP Performance Metrics (IPPM) [15] dan ITU-T Y.1540 IP packet transfer delay (IPTD) [14], yaitu delay antara titik pengukuran antara sumber dan tujuan untuk setiap paket yang berhasil dan error yang melewati jaringan adalah 150 milisecon, sedangkan delay yang didapat hanya sebesar 8.125 milisecon, sehingga pengiriman dari jaringan VPN IP tersebut dalam kategori sangat bagus.

A. Mengukur Parameter QOS (Quality Of Service) Video Streaming Dengan Menggunakan Wireshark

1. Bandwidth

Berikut adalah nilai bandwidth hasil capture menggunakan Wireshark pada Video Streaming :



Gambar 19. Grafik Bandwidth pada subnet 192.168.100.20/24

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	193100	193100	100.000%	0	0.000%
Between first and last packet	1935.803 sec				
Avg. packets/sec	99.752				
Avg. packet size	903.433 bytes				
Bytes	174452913	174452913	100.000%	0	0.000%
Avg. bytes/sec	90119.142				
Avg. MBit/sec	0.721				

Gambar 20. Summary

Dari simulasi yang dilakukan, hasil capture di atas menunjukkan bandwidth yang dihasilkan sebesar 0.721 Mbit/sec. Nilai ini cukup besar untuk simulasi layanan video streaming pada jaringan VPN IP. Dimana dalam kondisi real di Indonesia rata – rata bandwidth yang dihasilkan tidak lebih dari 1 - 1.5 Mbit/sec.

2. Bit Rate

Bit Rate adalah jumlah rata –rata nilai bit yang diperlukan untuk mengirimkan data dalam satuan waktu tertentu. Berikut hasil capture menurut wireshark :

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	193100	193100	100.000%	0	0.000%
Between first and last packet	1935.803 sec				
Avg. packets/sec	99.752				
Avg. packet size	903.433 bytes				
Bytes	174452913	174452913	100.000%	0	0.000%
Avg. bytes/sec	90119.142				
Avg. MBit/sec	0.721				

Gambar 21. Summary

Pada gambar 21. diatas nilai rata-rata yang dihasilkan untuk mengirimkan paket sebanyak 193100 adalah sebesar 90119.142 Bytes/sec atau 90.11 KB/Sec. Jika dikonversi kedalam Bit/sec untuk menyatakan kecepatan rata-rata transfer adalah sebagai berikut :

Bit Rate = 90.11 Kilobyte/sec x 8
= 720 kbps

Semakin tinggi bitrate, semakin bagus suara dan video yang dihasilkan, tetapi juga dibutuhkan kecepatan koneksi internet yang lebih tinggi.

3. Delay

Delay adalah waktu yang dibutuhkan untuk mentransmisikan data sampai ke penerima.

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	193100	193100	100.000%	0	0.000%
Between first and last packet	1935.803 sec				
Avg. packets/sec	99.752				
Avg. packet size	903.433 bytes				
Bytes	174452913	174452913	100.000%	0	0.000%
Avg. bytes/sec	90119.142				
Avg. MBit/sec	0.721				

Pada gambar 22. diatas diperlukan waktu untuk mengirimkan paket data sebanyak 193100 dari server ke client adalah 1935.803 sec. Sehingga dapat dihitung besar delay perpaket yang terjadi dengan persamaan berikut :

$$\text{Delay} = \frac{\text{Waktu Pengiriman}}{\text{Total paket data yang diterima}}$$

$$= \frac{1935.803}{193100}$$

$$= 0.01 \times 10^{3} = 10 \text{ milisecon}$$

Berdasarkan hasil simulasi video streaming pada jaringan VPN IP dapat disimpulkan bahwa dari hasil pengujian video streaming diketahui nilai delay menggunakan bitrate 720 kbps kurang dari 150 ms. Nilai delay tersebut masuk dalam kategori excellent berdasarkan ITU-T G.1010 [16].

B. Kelebihan dan Kekurangan membangun jaringan VPN IP

Beberapa kelebihan dan kekurangan dalam membangun jaringan VPN IP menggunakan GNS3 sebagai simulasi, sebagai berikut :

Keuntungan membangun jaringan VPN IP dengan menggunakan GNS3 :

1. Simulasi ini dapat menjadi bahan pembelajaran bagi para Engineer Muda yang ingin mempelajari jaringan VPN IP.
2. Kesalahan yang terjadi tidak menimbulkan kerugian.
3. Waktu dan tempat yang menjadi fleksibel untuk mempelajari jaringan VPN IP.
4. Penggunaan perangkat yang minim sehingga para Engineer Muda dapat dengan mudah mempelajari dan mempraktekannya.
5. Simulator GNS3 memiliki layanan untuk menghubungkan jaringan virtual yang telah dibangun dengan perangkat jaringan yang real.

Kerugian membangun jaringan VPN IP dengan menggunakan GNS3 :

1. Hasil perhitungan parameter-parameter yang berbeda dengan kondisi real.
2. Memory yang diperlukan lebih besar dikarenakan menggunakan memory RAM untuk menjalankan IOS Router 7200.

3. Hasil yang didapat sangat dipengaruhi oleh spesifikasi perangkat yang digunakan.
4. Kapasitas dari processor sangat mempengaruhi kestabilan kinerja IOS Router.

V. PENUTUP

5.1 Kesimpulan

Kesimpulan yang didapat dari penulis dari simulasi jaringan VPN IP menggunakan simulator GNS3 ini adalah :

1. Simulasi VPN IP yang dapat diterapkan untuk bahan pembelajaran berjalan dengan baik dan sudah sesuai dengan standarisasi yang ada.
2. Bandwidth yang dihasilkan pada saat pengiriman paket data di Client yang berada pada subnet 192.168.100.20/24 adalah sebesar 0.882 Mbps.
3. Bandwidth yang dihasilkan pada saat Video Streaming di Client yang berada pada subnet 192.168.100.20/24 adalah sebesar 0.721 Mbps.
4. Nilai bandwidth yang dihasilkan cukup besar untuk simulasi ini, dimana nilai bandwidth dalam kondisi real di beberapa institusi/perusahaan yang menggunakan jaringan VPN IP adalah tidak lebih dari 1,5 MB. Ada beberapa faktor yang mempengaruhi kualitas bandwidth pada simulasi ini, yaitu karakteristik dari perangkat yang digunakan untuk simulasi memiliki spesifikasi yang tidak cukup tinggi sehigga mempengaruhi kinerja dari pengiriman data, media transmisi yang digunakan juga mempengaruhi. Pada simulasi ini media transmisi yang digunakan adalah kabel UTP yang kapasitasnya hanya 100 MB sedangkan dalam kondisi real media transmisinya adalah kabel fiber optik yang kapasitasnya mencapai 1000 Mb (1 Gb).
5. Kecepatan transfer berdasarkan capture wireshark berjalan sangat stabil, tidak mengalami collusion data hal ini disebabkan perangkat yang digunakan memiliki spesifikasi dan kapasitas yang hampir sama satu sama lain. Misal tiga PC yang digunakan dengan processor AMD, kapasitas memory (RAM) sebesar 4 GB & 8 GB dan adapter LAN dengan kapasitas 1 Gb.
6. Delay yang dihasilkan pada saat pengiriman paket data sangat bagus yaitu sebesar 8,125 ms. Dimana menurut standar IETF dan ITU rata-rata delay yang bagus untuk pengiriman paket data menggunakan TCP dan HTTP adalah 150 ms.
7. Delay yang dihasillkan pada simulasi video streaming diketahui menggunakan bitrate 720 kbps kurang dari 150 ms. Nilai delay tersebut masuk dalam kategori excellent berdasarkan ITU-T G.1010.

5.2 Saran

1. Aktifkan idle PC pada masing-masing router saat mengaktifkan router pada GNS3, untuk penghematan daya RAM.
2. Sebelum mengaktifkan router di GNS3, pastikan adapter LAN sudah terpasang dan sudah tersetting agar konfigurasi pada GNS3 dapat membaca adapter saat pengaktifan.
3. RAM pada PC yang digunakan harus berkapasitas besar.
4. Gunakan adapter LAN gigabit ethernet jika jumlah port LAN pada PC tidak cukup.
5. Pastikan antivirus dan firewall dalam kondisi off pada saat menjalankan simulasi.

DAFTAR PUSTAKA

1. Pengertian gns3 (by didha dewannanta) dari ilmukomputer.org/wp-content/uploads/2013/01/gns3.pdfdi akses pada tanggal 12 Mei 2014
2. VPN IP http://www.freewebs.com/andromedasilver/Paper%20VPN.doc. diunduh pada 14 mei 2014.
3. VPN IP darihttp://thiramahari.files.wordpress.com/2011/06/tugas-vpn.pdf. Diakses pada tanggal 15 Mei 2014
4. Sistem Keamanan VPN dari http://kambing.ui.ac.id/onnopurbo/library/library-ref-ind/ref-ind-3/network/VPN_jurnal.pdf. Di Unduh pada tanggal 15 Mei 2013.
5. Standar Delay ITU-T http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC- Y.1540-201103-I!!PDF-E&type=items. Di akses pada tanggal 6 Juli 2014
6. Standar Delay IETF http://tools.ietf.org/html/rfc3393 di akses pada tanggal 6 Juli 2014
7. Kwok, Shneiderman, Gallaway, dkk., 2001, ITU-T Recommendation G.1010, http://itu.int/. Diakses tanggal 6 Juli 2014.

Gambar 21. Sum