Analisis Jaringan VPN Protokol SSTP Pada Video Stream

Rizaldi Muflih Santoo
Program Studi Teknik Multimedia dan Jaringan,
Jurusan Teknik Informatika dan Komputer,
Politeknik Negeri Jakarta
Jl. Prof. DR. G.A. Siwabessy, Kampus UI, Depok 16425
Telp: (021)91274097, Fax : (021) 7863531, (021)7270036

Email : rizaldimuflihs30@gmail.com

Abstrak – Penelitian ini berfokus pada pengujian dan menganalisa Jaringan VPN SSTP pada video stream. Seiring meningkatnya kebutuhan pertukaran informasi antar perusahaan maka diperlukan metode yang lebih baik, cepat, dan aman. Internet adalah salah satu metode yang saat ini banyak digunakan. Komunikasi data melalui jaringan internet mengakibatkan masalah kecepatan transfer dan keamanan . Internet telah menyediakan akses untuk layanan telekomunikasi dan sumber daya informasi untuk jutaan penggunanya yang tersebar di seluruh dunia. Adapun layanan yang tersedia yaitu E-Mail (Electronic Mail), E-Commerce, E-Banking, E-Learning, E-Government, Milist (Mailing List), IRC (Internet Relay Chat), VOIP (Voice Over Internet Protocol). Rumusan masalah pada penelitian ini adalah bagaimana mensimulasikan jaringan VPN dengan protokol SSTP di dalam sebuah virtual machine (VM) yang berjalan pada server fisik yang sama? Untuk menjawab rumusan masalah tersebut maka tujuan dari penelitian ini yaitu dapat mensimulasikan jaringan VPN tersebut dengan menggunakan server fisik yang sama (hardware). Tujuan dari penelitian ini adalah untuk menganalisa hasil kinerja jaringan menggunakan parameter QoS (Quality of Service). Penelitian ini dilakukan pengujian koneksi antara client-server dan melakukan streaming dari sisi client dengan mengamati parameter QoS salah satu nya adalah latency saat dilakukannya pengujian sehingga dapat dianalisa hasilnya.

Kata kunci** – **Jaringan, VPN, SSTP

I. PENDAHULUAN

Seiring meningkatnya kebutuhan pertukaran informasi antar perusahaan maka diperlukan metode yang lebih baik, cepat, dan aman. Internet adalah salah satu metode yang saat ini banyak digunakan. Komunikasi data melalui jaringan internet mengakibatkan masalah kecepatan transfer dan keamanan .

Internet telah menyediakan akses untuk layanan telekomunikasi dan sumber daya informasi untuk jutaan penggunanya yang tersebar diseluruh dunia. Adapun layanan yang tersedia adalah E-Mail (Electronic Mail), E-Commerce, E-Banking, ELearning, E-Government, Milist (Mailing List), IRC (Internet Relay Chat), VOIP (Voice Over Internet Protocol).(Saroji et al., 2021)

Hal yang harus diperhatikan dalam melakukan kegiatan di dunia internet adalah semakin banyak orang yang berusaha untuk mencuri data-data penting kita Akan tetapi permasalahan yang sering timbul adalah faktor keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Oleh karena itu lah VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman. Dalam sebuah jaringan komputer, keamanan sewaktu pengiriman dan penerimaan data sangat penting untuk menjamin bahwa data yang dikirim sampai pada yang pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan, terutama apabila data yang dikirimkan tersebut bersifat rahasia.

Namun, terkadang disaat traffic *bandwidth* jaringan yang besar dapat menyebabkan adanya *delay* di jaringan tersebut Solusi agar sebuah IP yang terhubung dapat mengirimkan data agar tidak mengganggu jaringan lainnya ialah dengan Tunneling diantara kedua jaringan tersebut. Metode Tunneling merupakan metode yang mampu menghubungkan keduanya. Tunnel merupakan kanal dalam pengalamatan Internet Protocol diantara dua jaringan komputer yang digunakan untuk transportasi menuju jaringan yang lain dengan mengkapsulkan paket- paket di dalamnya.

VPN (Virtual Private Network) adalah sebuah teknologi komunikasi yang memungkinkan untuk terkoneksi ke jaringan publik dan menggunakanya untuk bergabung ke jaringan lokal, dengan cara tersebut maka akan diperoleh hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau jaringan itu sendiri, walaupun sebenarnya menggunakanjaringan publik. Jaringan VPN merupakan jaringan yang dibangun di atas sebuah tunnel. (Zamalia et al., 2018)

tunnel vpn mempunyai fungsi sebagai lajur lalu lintas yang bertanggung jawab atas keamanan dari data yang berada di dalamnya. Adapun untuk pengujian performa dilakukan menggunakan beberapa parameter QoS (Quality of Service) untuk memperoleh kualitas dari keempat tunnel dan pengujian keamanan dilakukan dengan cara meretas sistem keamanan tunnel.Proses enkripsi dan dekripsi pada VPN membuat delay di dalam jaringan bertambah karena proses ini juga membutuhkan waktu yang pada akhirnya akan berpengaruh pada hasil performansi QoS (Quality of service) dari jaringan vpn tersebut.

II. TINJAUAN PUSTAKA

A. *Jaringan Komputer*

Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di Laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian.

Di tahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem Time Sharing System (TSS) beberapa terminal terhubung secara seri kesebuah host komputer. Dalam proses Time Sharing System (TSS) mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hamper seluruh aplikasi jaringan komputer.

B. *Jaringan VPN (Virtual Private Network)*

VPN merupakan suatu koneksi antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan internet. Pengguna dapat mengirim dan menerima data melalui jaringan bersama atau public seakan perangkat komputasi mereka langsung terhubung ke jaringan pribadi, dan dengan demikian mendapatkan keuntungan dari fungsi, keamanan dan manajemen kebijakan dari jaringan pribadi (*private network*).

Secara singkat, VPN merupakan saluran komunikasi khusus yang efisien menggunakan jaringan internet. Fungsi dari VPN adalah memberikan koneksi yang aman antara jaringan pribadi yang terhubung melalui internet.

C. *Teknologi Tunneling pada VPN*

Tunnel VPN memiliki fungsi sebagai jalur yang bertanggung jawab atas keamanan dari data yang berjalan di dalamnya. Pengujian dilakukan dengan cara membandingkan performa dan keamanan masing-masing tunnel. Pengujian performa dilakukan menggunakan beberapa parameter QoS (Quality of Service) untuk memperoleh kualitas dari keempat tunnel dan pengujian keamanan dilakukan dengan cara meretas sistem keamanan tunnel.

Proses enkripsi dan dekripsi pada VPN membuat delay di dalam jaringan bertambah karena proses ini juga membutuhkan waktu. Keamanan data pada VPN pada akhirnya akan berpengaruh pada performansi QoS (Quality of service).

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah dibuat. Dalam artian antara sumber *tunnel* dengan tujuan *tunnel* telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun.

D. *Secure Socket Tunneling Protocol (SSTP)*

Secure Socket Tunneling Protocol (SSTP) adalah bentuk VPN tunnel yang menyediakan mekanisme untuk mengirimkan traffic PPP atau L2TP melalui sebuah saluran SSL 3.0. SSL menyediakan transport-level security dengan key-negotiation, enkripsi dan traffic integrity checking. Penggunaan SSL melalui port TCP 443 mengizinkan SSTP untuk melewati secara virtual semua firewall dan proxy server kecuali untuk otentikasi web proxy.

SSTP ini adalah salah satu protocol VPN yang mempunyai kombinasi dua teknologi yaitu SSL (*Secure Socket* Layer) dan TCP (*Transmission Control Protocol*). Secara keseluruhan protocol ini adalah salah satu yang pilihan terbaik dikarenakan stabil dan mudah digunakan dalam menyelesaikan masalah konektivitas yang ada.

E. *QoS (Quality of Service)*

Merupakan kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan kapasitas jaringan, mengatasi jitter dan delay (waktu tunda). QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Terdapat banyak hal bisa terjadi pada paket Ketika melakukan perjalanan dari asal ke tujuan, yang mengakibatkan masalah-masalah dan sering disebut sebagai parameter-parameter QoS, antara lain:

- ***Delay*** **(Waktu tunda)**

Merupakan akumulasi berbagai waktu tunda dari ujung ke ujung pada jaringan Internet. *Delay* mempengaruhi kualitas layanan (QoS) karena waktu tunda menyebabkan suatu paket lebih lama mencapai tujuan.

- ***Jitter*** **(Variasi Waktu Tunda)**

Merupakan perbedaan selang waktu kedatangan antar paket di terminal tujuan. *Jitter* dapat disebabkan oleh terjadinya kongesti, kurangnya kapasitas jaringan, variasi ukuran paket, serta ketidakurutan paket.

- ***Packet Loss*** **(Paket Hilang)**

Merupakan penyebab utama pelemahan audio dan video *streaming*, VoIP dan *Conference Call*. *Packet Loss* dapat disebabkan oleh pembuangan paket di jaringan *(network loss)* atau pembuangan paket di *gateway*/terminal sampai kedatangan terakhir (*late loss*). *Network loss* secara normal

disebabkan kemacetan *(router buffer overflow)*, perubahan rute secara seketika, kegagalan *link dan lossy link* seperti saluran nirkabel. Kemacetan atau kongesti pada jaringan merupakan penyebab utama dari *packet loss.*

- ***Throughput***

  Merupakan *rate* (kecepatan) transfer data efektif, yang diukur dalam *bit per second* (bps). *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada sisi klien/tujuan selama selang waktu tertentu dibagi oleh durasi selang waktu tersebut.

F. VMware Workstation

VMware adalah sebuah program komputer under Windows dari perusahaan Bernama VMware yang merupakan sebuah tool atau program virtualisasi yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" didalam sistem operasi "utama", dengan kata lain sebuah sistem operasi didalam sistem operasi tanpa harus mengganggu sistem utama yang sudah ada. Virtualisasi yang dimaksud adalah membuat mesin pc virtual yang bisa berjalan secara independen diatas sistem operasi utama.

III. METODOLOGI

A. Rancangan Penelitian

Dalam penelitian ini penulis menggunakan metode penelitian kualitatif yang bersifat studi Pustaka dan observasi.

1. **Cara kerja sistem**

Pada topologi ini, semua perangkat dibuat untuk tidak saling terhubung antar device hanya dibuat agar bisa terhubung dengan server. Penggunaan routing OSPF dalam topologi ini membuat router dan server bisa saling terhubung dan menggunakan pengaturan IP *static* pada semua perangkat, OSPF ini berfungsi sebagai *dynamic routing* agar dapat menyesuaikan routing yang ada secara otomatis karena pada simulasi ini terdapat beberapa segment IP yang berbeda.

Pada akhirnya client dan server dapat terhubung langsung.

2. **Spesifikasi Perangkat Lunak dan Keras**

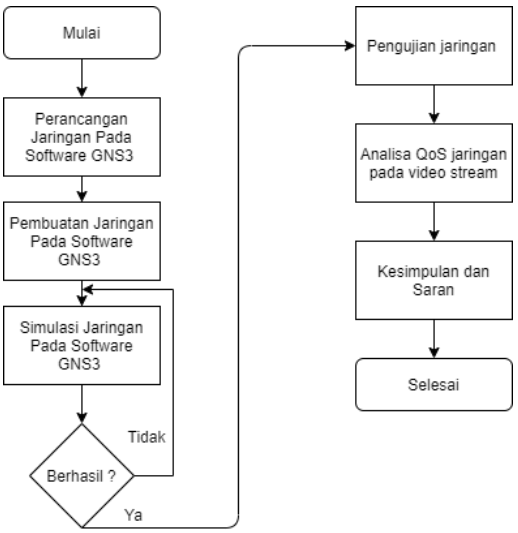
Untuk merancang tugas akhir ini ada beberapa perangkat yang dibutuhkan supaya perancangan yang sudah dibuat dapat diimplementasikan. Penentuan perangkat yang dibutuhkan ini harus sesuai dengan kebutuhan yang akan dibuat nanti, kebutuhan tersebut meliputi perangkat lunak (hardware) dan keras (software).

NO	Perangkat	Spesifikasi
1.	Laptop	Asus A450L, processor i7 – 4500u dengan RAM 6 GB dan berjalan di dalam sistem operasi Windows 10
2.	IOS	Mikrotik
IOS MIKROTIK		
3.	IOS Router	Mikrotik 6.34
Software		
4.	*Graphic Network Simulator* 3	GNS3-2.2.28-all-in-one-regular
5.	*Virtual Machine*	VMware-workstation-pro-16

B. Tahapan Penelitian

1. Alur Penelitian

Pada bab ini akan membahas tentang tahapan-tahapan yang dilakukan dalam penelitian. Langkah pertama yang dilakukan adalah perancangan sistem, berikut adalah diagram sistem yang akan dipakai.



- Perancangan jaringan pada software gns3 :

  yaitu sebuah proses untuk merancang sebuah jaringan baik secara fisik atau secara logic tapi pada proses ini yaitu memakai secara logic. Dalam tahap ini adalah membuat topologi jaringan yang akan dipakai

- Pembuatan jaringan pada software gns3 :

  setelah topologi jaringannya sudah dibuat maka selanjutnya adalah menkonfigurasi jaringan nya agar siap dilakukan nya simulasi.

- Simulasi jaringan pada software gns3 :

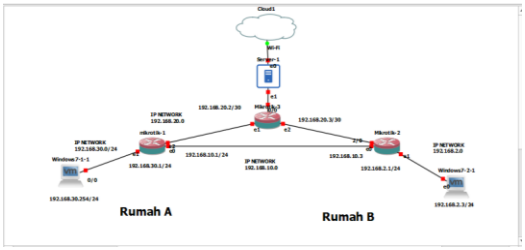
  Pada tahap ini jaringan yang sudah dibuat tadi akan diuji koneksinya apakah sudah bisa terhubung dan sesuai dengan apa kita rancang sebelumnya . Jika berhasil maka akan masuk ke tahap selanjutnya namun, jika disaat pengujian terdapat error atau ada kesalahan maka akan balik ke pembuatan jaringan.

- Pengujian jaringan pada software gns3 :

  Jika sudah terhubung semua jaringan nya maka selanjutnya akan diuji dengan parameter *qos (quality of services).*

3. **Topologi Jaringan**

   Topologi yang dibuat pada Analisa jaringan vpn protocol SSTP (*Secure Socket Tunneling Protocol*) pada video stream ini membentuk sebuah bentuk topologi *tree*. Di dalam topologi ini terdapat 3 router, 2 client, dan 1 server, kebutuhan dalam jaringan ini adalah bisa menonton video dari server di sisi client melalui koneksi VPN. Maka dari itu, antar client tidak dirancang untuk saling terhubung dalam hal ini diasumsikan sebagai "rumah A" dan "rumah B". *Routing protocol* yang akan diimplemtasikan pada router adalah OSPF (*Open Shortest Path First*) dan *routing static*. Berikut adalah gambar dari topologi jaringan nya.



C. Objek Penelitian

Topologi yang sudah dibuat maka akan diberikan ip untuk setiap interface yang ada sesuai dengan kebutuhan.

1. ***Inisialisasi Interface Jaringan***

Dalam perancangan jaringan tersebut terdapat beberapa segmen IP yang berbeda yaitu, /24 untuk area client dan /30 untuk area antar router. /30 yang dipakai ini diperuntukan khusus untuk distribution layer dan /24 diperuntukkan untuk access layer, Inisialisasi interface jaringan ini diperlukan untuk pengalamatan pada setiap interface. Berikut merupakan table dari inisialisasi alamat pada setiap interface.

No	Bagian	*Interface*	*IP Address*	*Network ID*	*Prefix*	*Subnetmask*
1	R1	E1	192.168.10.1	192.168.10.0	24	255.255.255.0
		E2	192.168.30.1	192.168.30.0	24	255.255.255.0
		E3	192.168.20.1	192.168.20.0	30	255.255.255.0
		lo0	1.1.1.1	1.1.1.1	30	255.255.255.0
2	R2	E1	192.168.10.3	192.168.10.0	24	255.255.255.0
		E2	192.168.2.1	192.168.2.0	24	255.255.255.0
		E3	192.168.20.4	192.168.20.0	30	255.255.255.0
		lo0	2.2.2.2	2.2.2.2	30	255.255.255.0
3	R3	E1	192.168.0.1	192.168.0.0	24	255.255.255.0
		E2	192.168.20.2	192.168.20.0	30	255.255.255.0
		E3	192.168.20.3	192.168.20.0	30	255.255.255.0
		lo0	3.3.3.3	3.3.3.3	30	255.255.255.0
4	Client 1	E1	192.168.30.254	192.168.30.0	24	255.255.255.0
5	Client 2	E1	192.168.2.3	192.168.2.0	24	255.255.255.0
6	Server	E1	192.168.220.3	192.168.220.0	24	255.255.255.0
		E2	192.168.0.4	192.168.0.0	24	255.255.255.0

2. ***Konfigurasi Jaringan***

Pada perancangan jaringan mensimulasikan 2 jaringan dalam satu topologi, di bagian area backbone dilakukan konfigurasi OSPF dan Static Routing. Setelah simulasi pengujian dapat berjalan dengan baik lalu dilakukan Analisa menggunakan wireshark dan didapatkan hasil parameter QoS untuk mengetahui hasil kinerja jaringan nya. Adapun konfigurasi yang dilakukan terhadap topologi pada gambar 3.2.2 adalah sebagai berikut :

- *Konfigurasi Interface*

  Konfigurasi yang dilakukan terhadap beberapa image terdapat dua interface yaitu interface ethernet dan interface loopback

Konfigurasi loopback R1

R1> interface bridge add name=bridge1

R1> ip addresses add address=1.1.1.1/30 interface=bridge1

Konfigurasi loopback R2

R2> interface bridge add name=bridge1

R2> ip addresses add address=2.2.2.2/30 interface=bridge1

Konfigurasi loopback R3

R3> interface bridge add name=bridge1

R3> ip addresses add address=3.3.3.3/30 interface=bridge1

Konfigurasi Ethernet di R1

R1> ip addresses add address=192.168.10.1/24 interface=ether1

R1> ip addresses add address=192.168.30.1/24 interface=ether2

R1> ip addresses add address=192.168.20.1/30 interface=ether3

R1> ip addresses print

R1> ip route add dst-address=3.3.3.3/30 gateway=192.168.20.1

Konfigurasi Ethernet di R2

R2> ip addresses add address=192.168.10.3/24 interface=ether1

R2> ip addresses add address=192.168.2.1/24 interface=ether2

R2> ip addresses add address=192.168.20.4/30 interface=ether3

R2> ip addresses print

R2> ip route add dst-address=3.3.3.0/30 gateway=192.168.20.4

Konfigurasi Ethernet di R3

R3> ip addresses add address=192.168.0.1/24 interface=ether1

R3> ip addresses add address=192.168.20.2/30 interface=ether2

R3> ip addresses add address=192.168.20.3/30 interface=ether3

R3> ip addresses print

R3> ip route add dst-address=1.1.1.0/30 gateway=192.168.20.2

R3> ip route add dst-address=2.2.2.0/30 gateway=192.168.20.3

- *Konfigurasi OSPF*

  Untuk konfigurasi Routing OSPF yang sudah seperti diberitahukan sebelumnya , ini adalah salah satu protocol yang digunakan dalam penelitian. Routing OSPF mempunyai prinsip kerja yaitu memberi jalur paket data berdasarkan jarak terdekat, jarak terdekat yang dimaksud adalah router akan memilih jalur yang mempunyai nilai cost terbaik (dalam perhitungan metric). Berikut ini adalah cara konfigurasi routing protocol OSPF.

Konfigurasi OSPF di R1

R1> routing ospf interface add interface=ether3

R1> routing ospf instance set default router-id=0.0.0.1

R1> routing ospf network add network=192.168.30.0/24 area=backbone

R1> routing ospf network add network=192.168.10.0/24 area=backbone

R1> routing ospf network add network=192.168.20.0/30 area=backbone

Konfigurasi OSPF di R2

R2> routing ospf interface add interface=ether3

R2> routing ospf instance set default router-id=0.0.0.2

R2> routing ospf network add network=192.168.10.0/24 area=backbone

R2> routing ospf network add network=192.168.2.0/24 area=backbone

R2> routing ospf network add network=192.168.20.0/30 area=backbone

Konfigurasi OSPF di R3

R3> routing ospf interface add interface=ether2

R3> routing ospf interface add interface=ether3

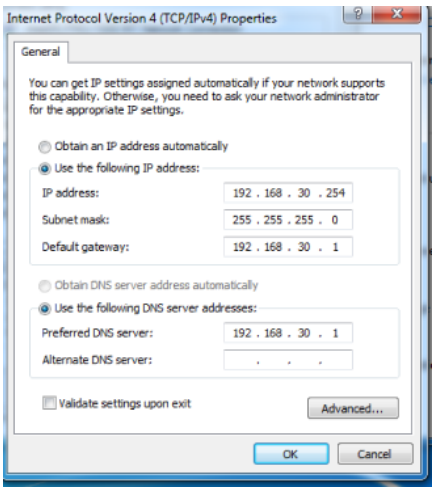
R3> routing ospf instance set default router-id=0.0.0.3

R3> routing ospf network add network=192.168.0.0/24 area=backbone

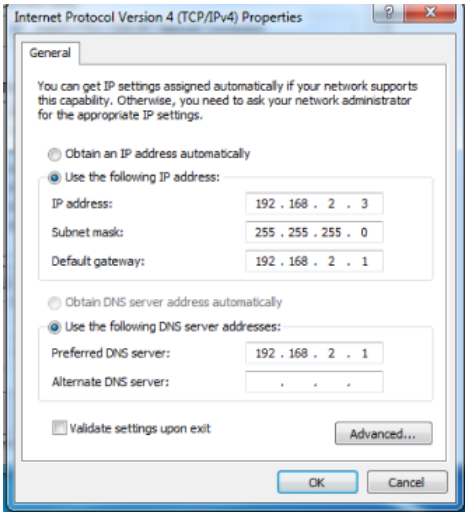
R3>routing ospf network addc network=192.168.20.0/30 area=backbone

- *Konfigurasi Client*

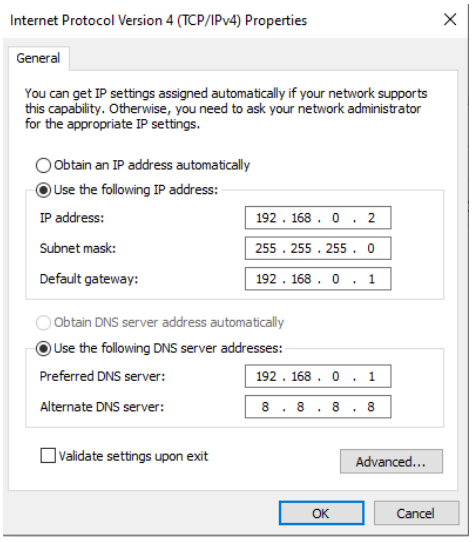
  Alamat IP address yang terdapat pada computer di konfigurasi secara static yang terkoneksi dengan router masing-masing.



Gambar 3.3 IP Address Client 1

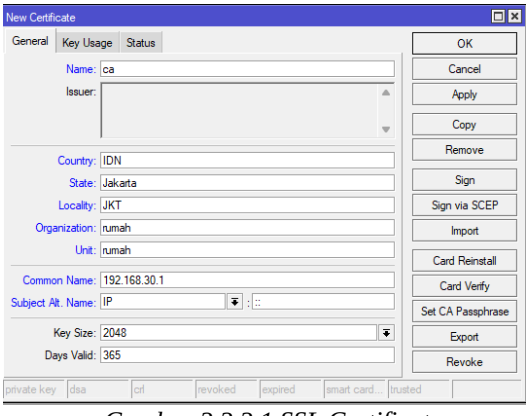


Gambar 3.4 IP Address Client 2



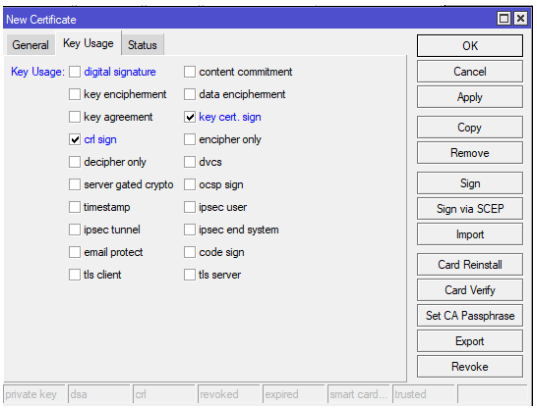
Gambar 3.5 IP Address Server

- *Konfigurasi SSL certificate*
  Untuk terwujudnya simulasi jaringan VPN dengan protocol SSTP ini diperlukan adanya SSL Certificate (Secure Socket Layer), SSL ini adalah sebuah protocol kriptografi yang mempunyai fungsi sebagai pengamanan dalam mengkomunikasikan data dan bertujuan memberikan privasi dan integritas data antara dua atau lebih perangkat yang berkomunikasi.



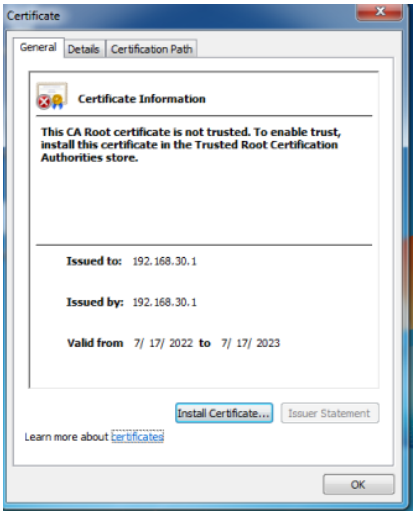
Gambar 3.3.3.1 SSL Certificate

Berikut adalah konfigurasi certificate yang dipakai dan SSL ini didapatkan melalui fitur di mikrotikOS yaitu terdapat pada menu System -> Certificate



Gambar 3.3.3.2 SSL Certificate

Pada bagian Key Usage pilih opsi crl sign dan key cert. sign yang berfungsi untuk memudahkan saat berkomunikasi jika sudah jangan lupa untuk memvalidasi certificate tersebut agar bisa terindetifikasi sebagai trusted.



Gambar 3.3.3.3SSL Certificate

Selanjutnya adalah menginstall SSL certificate nya yang sudah dibuat sebelumnya, certificate ini diinstal pada perangkat-perangkat yang nantinya akan saling berkomunikasi.

IV. PEMBAHASAN

A. *Pengujian*

Jaringan simulasi VPN yang dapat dikatakan berjalan atau tidak dengan melaksanakan test ping dari sisi client ke server.

- *Vertifikasi Routing Static*

  Routing yang digunakan pada router adalah static. Routing tersebut dapat terbentuk atau tidaknya dengan cara melihat apakah berjalan atau tidak di console. Berikut hasilnya

```
[admin@MikroTik] > ping 192.168.20.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.20.1                               56  64 0ms
    1 192.168.20.1                               56  64 0ms
    2 192.168.20.1                               56  64 0ms
    3 192.168.20.1                               56  64 0ms
    sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Gambar 4.1.1 Router R1

```
[admin@MikroTik] > ping 192.168.10.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.10.1                               56  64 0ms
    1 192.168.10.1                               56  64 0ms
    2 192.168.10.1                               56  64 0ms
    3 192.168.10.1                               56  64 0ms
    4 192.168.10.1                               56  64 0ms
    sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Gambar 4.1.2 Router R1

Disini penulis melakukan pengujian koneksi antara router 1 – router 3 dan client dengan size packet yang sama yaitu 56 kb dan hasilnya berhasil terkoneksi dan terkirim ke tujuan dengan baik tanpa adanya packet loss

- *Vertifikasi Routing OSPF*

  Routing yang digunakan pada router adalah OSPF. Routing tersebut dapat terbentuk atau tidaknya dengan cara melihat apakah berjalan atau tidak di console. Berikut hasilnya.

```
[admin@MikroTik] > interface bridge add name=loopback
[admin@MikroTik] > ip address add address=1.1.1.1/30 interface=loopback
[admin@MikroTik] > routing ospf instance set 0 router-id=1.1.1.1 distribute-defa
ult=always-as-type-1
no such item
```

Gambar 4.1.13 Hasil dari *routing ospf* Router

Namun saat dilakukan pengaktifkan routing OSPF terdapat kendala yaitu tidak bisa diaktifkan karena terbatas pada level license yang di dapat yang mengharuskan mempunyai license minimal yaitu level 4.

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	do not sell	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

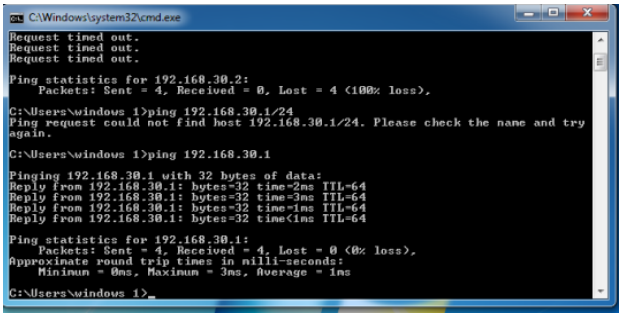
Gambar 4.1.14 Perbandingan level license mikrotik (Sumber : https:// belajarmikrotik.com/)

B. *Deskripsi Pengujian*

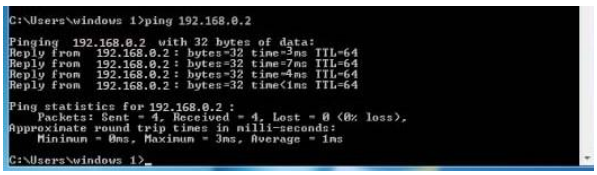
Pengujian dilakukan setelah table routing selesai, dengan menggunakan konfigurasi routing static dan OSPF. Pada setiap rumah melakukan test ping pada client dan server jika sudah berhasil, selanjutnya adalah mengkoneksikan vpn client dengan vpn server yang sudah dibuat dan proses selanjutnya adalah memutar video (streaming) dari sisi client.

C. *Prosedur Pengujian*

Routing protocol yang telah dikonfigurasikan adalah static dan OSPF. Untuk mengetahui apakah sudah terhubung maka dilakukan pengetesan yaitu ping, test ping yang dilakukan yaitu berkomunikasi antara client-router dan client-server. Jaringan yang telah dibuat dalam topologi analisis ini adalah static dan OSPF. Berikut adalah hasil dari test ping dari tiap client.



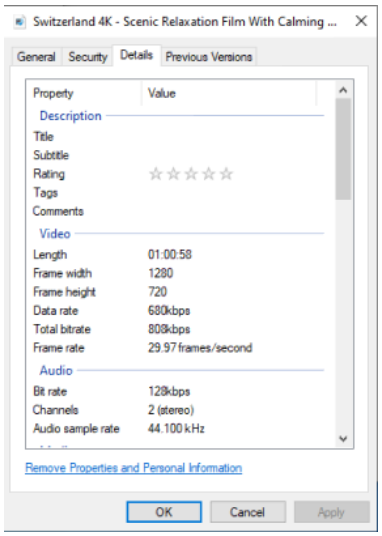
Gambar 4.3.1 Hasil dari test ping ke router



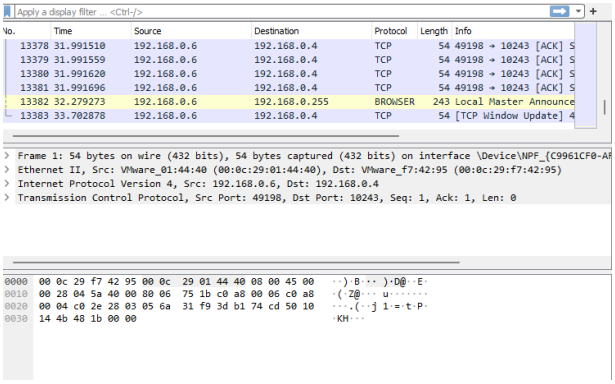
Gambar 4.3.2 Hasil dari test ping ke server

D. *Data Hasil Pengujian*

Pengujian yang telah dilakukan sebelumnya yaitu adalah berupa pengetesan ping antar perangkat router dan server, yang mempunyai fungsi untuk mengecek apakah konfigurasi yang sudah dibuat ini berhasil atau tidak.

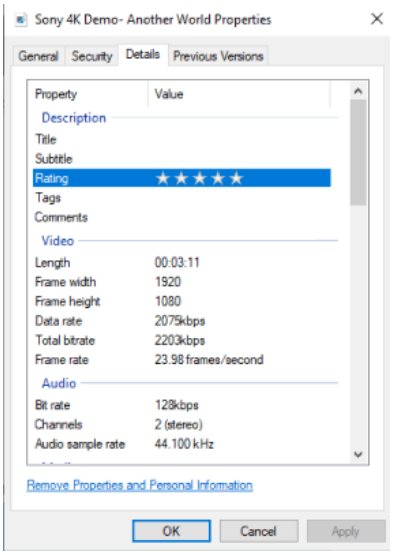


Gambar 4.4.1 Sample video 1 pengetesan

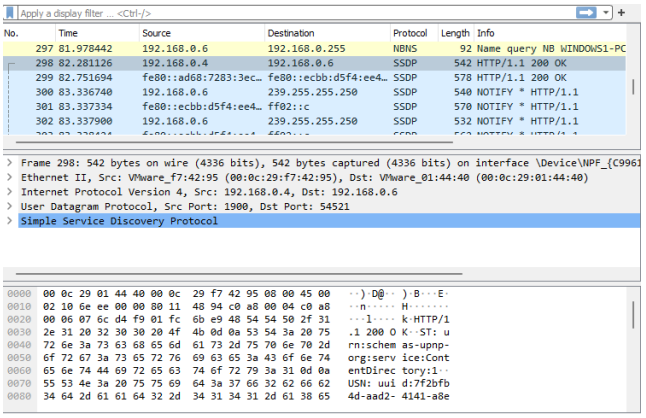


Gambar 4.4.2 Hasil dari capture stream video beresolusi HD di server

Hasil capture wireshark yang terdapat diatas merupakan bentuk pengujian yaitu stream video yang dilakukan pada sisi client ke sisi server dan didapatkan hasil dengan rata-rata latency 31,9 ms dengan sample video berdurasi 60 menit di resolusi 720p HD. Dan selanjutnya akan dilakukan pengetesan yang kedua, berikut adalah hasil pengetesan nya.



Gambar 4.4.3 Sample video 2 pengetesan



Gambar 4.5 Hasil dari capture stream video beresolusi Full HD di server

Dan setelah dilakukan pengetesan kedua dengan sample video berdurasi 3 menit 11 detik dan beresolusi 1080p Full HD terlihat hasil yang berhasil di capture oleh aplikasi wireshark yang mempunyai rata-rata latency 83 m

V. KESIMPULAN

Berdasarkan dari hasil pengujian yang dilakukan untuk menganalisa jaringan VPN SSTP pada video stream dapat disimpulkan sebagai berikut :

1. Static, digunakan untuk memberikan pengalamatan pada perangkat yang akan digunakan untuk berkomunikasi dari satu perangkat menuju perangkat lainnya.
2. OSPF, mempunyai fungsi sebagai membagikan jaringan berdasarkan salah satunya pengelompokan area yang menjadikan penyebaran datanya lebih teratur akan tetapi terdapat kendala yaitu level license sehingga fitur tersebut belum bisa digunakan
3. Protokol VPN SSTP, yang akan digunakan ini seharusnya bisa digunakan sebagai jalur tunnel yang dapat meningkatkan keamanan dalam berkomunikasi antar perangkat akan tetapi dalam penelitian ini seperti yang sudah diberitahukan mempunyai kendala pada level license yang membuat vpn ini hanya bisa terhubung dengan satu perangkat.

Dan didapati hasil pengujian dengan sampel video 1 yang berdurasi 60 menit beresolusi HD mendapatkan latency sebesar 31,9 ms, lalu untuk sampel video 2 yang mempunyai durasi 3 menit 11 detik dengan resolusi full HD mendapatkan latency sebesar 83 ms. Yang mana ini dapat dikategorikan sempurna karena <150 ms dan mengingat SSTP ini mempunyai keunggulan port yang digunakan oleh protocol SSTP ini dapat melewati seluruh firewall. Dengan begitu dapat disimpulkan jaringan VPN dengan Protokol SSTP ini bisa berjalan aman untuk kebutuhan streaming video.

VI. REFERENSI

[1] Mufida, E., Irawan, D., Chrisnawati, G. (2017). REMOTE SITE MIKROTIK VPN DENGAN POINT TO POINT TUNNELING PROTOCOL (PPTP) STUDI KASUS PADA YAYASAN TERATAI GLOBAL JAKARTA. Jurnal MATRIK, 16(2). 9-11.

[2] Afrianto, I., Setiawan, E.B. (2011). KAJIAN VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SISTEM PENGAMANAN DATA PADA JARINGAN KOMPUTER. Majalah Ilmiah UNIKOM, Program Studi Teknik Informatika, Universitas Komputer Indonesia, Bandung.

[3] Zamalia, W,O., Aksara, L.M., Yamin, M. (2018). ANALISIS PERBANDINGAN PERFORMA QoS, PPTP, L2TP, SSTP DAN IPSEC PADA JARINGAN VPN MENGGUNAKAN MIKROTIK. Jurnal semanTIK, 4(2).

[4] Nurhayati, A., Putri, S.A. (2019). SIMULASI TUNNELING IPV6 OVE IPV4. *Jurnal* ICT 1(1). 001-010

[5] Nurhayati, A., Pantoro, S.D. (2015). SIMULASI JARINGAN VPN BERBASIS MPLS DENGAN MENGGUNAKAN SOFTWARE OPNET MODULAR 14.5. Jurnal ICT 6(11). 38-43.

[6] Putri, M.A., Setiawan, I.W. (2019). PENERAPAN MODEL SIMULASI *ORACLE VIRTUALBOX* PADA KOMPETENSI SISTEM OPERASI DI SMK HIDAYAH SEMARANG. *Jurnal* Multimatrix 1(2). 5-11.

[7] Heryanto, V.P., Riza, T.A, Gaatot, S.T. (2019). SIMULASI DAN ANALISA QoS MULTIPROTOCOL LABEL SWITCHING UNTUK LAYANAN METRONET PADA JARINGAN PADA JARINGAN PT. INDONESIA COMNETS PLUS (ICON+). Jurnal e-proceeding of applied science 5(3). 3132-3142.

[8] Bambang, S., Suharyanto. (2019). Perancangan Jaringan VPN Menggunakan Metode Point to Point Tunneling Protocol. Jurnal Teknik Komputer 5(2). 235-240.