BAB II: TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1. Tinjauan Pustaka

Penelitian yang dilakukan oleh Lukman dan Aiman Mukhlishah pada tahun 2020 yang berjudul "Analisis Perbandingan Kinerja Jaringan *Secure Socket Tunneling Protocol* (SSTP) Dan *Layer Two Tunneling Protocol* (L2TP) + *Internet Protocol Security* (IPSec) Menggunakan Metode *Quality Of Service* (QoS)". Menurut peneliti masalah yang dihadapi saat ini yaitu ketika performa jaringan yang lambat akan berpengaruh pada kinerja perusahaan, untuk berhubungan antar kantor menggunakan internet dan *email* untuk mengirim data dan berkomunikasi maka dibutuhkan jaringan privat untuk memudahkan mengakses file terhadap suatu tempat yang berbeda lokasi. Namun dalam Pemilihan VPN yang akan digunakan memungkinkan kurang tepatnya pemilihan metode yang digunakan dalam mengelola jaringan intranet untuk perusahaannya. Dari uraian diatas maka penulis melakukan analisis perbandingan sebuah teknik tunneling dengan menggunakan SSTP dan L2TP+IPSec. SSTP dan L2TP+IPSec merupakan *protocol* jaringan yang dapat melindungi jaringan dari ancaman luar seperti konflik IP, MAC dan DHCP *server* jahat, serta membuat performa jaringan lebih baik, dengan metode penggunaan jalur tersendiri yang di lalui atau dilewati. Dari kedua metode tersebut penulis melakukan perbandingan performa jaringan ketika di terapkan metode SSTP dan L2TP+IPSec sehingga mengetahui performa jaringan mana yang lebih bagus dan cocok digunakan sesuai dengan kebutuhan pengguna. Hasil dari penelitian ini diharapkan dapat membantu siapapun untuk menentukan metode tunneling VPN yang akan digunakan kelak dalam suatu jaringan. Sedangkan dari hasil penelitian bisa diambil kesimpulan bahwa L2TP+IPSec lebih baik dibanding SSTP, dinilai dari parameter QOS yang sudah diuji dan dibandingkan [5].

Penelitian yang dilakukan oleh Dahnial pada tahun 2019 yang berjudul *"Analisa Perbandingan Quality Of Service Antara Protocol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik"*. Menurut peneliti internet sebagai *backbone* pengiriman data memiliki ancaman keamanan dalam pengiriman

data. Untuk mengatasi masalah keamanan setiap komunikasi data yang dilakukan melalui jaringan publik *(public network)* maka diperlukan suatu mekanisme yang memungkinkan koneksi antar *workstation* berjalan secara privat, sehingga hanya *workstation* yang memiliki akses yang dapat saling terhubung, dengan cara memanfaatkan *Virtual Private Network* (VPN). Terdapat dua *protocol* yang dapat dipilih dalam VPN yaitu *Point to Point Tunneling Protocol* (PPTP) dan *Layer 2 Tunneling Protocol* (L2TP). Akan tetapi belum diketahui performa dari masing – masing *protocol* tersebut. Untuk mengetahui kinerja dari kedua *protocol* tersebut diperlukan sebuah pengujian dengan metode simulasi. Menggunakan router mikrotik dan aplikasi Wireshark dengan parameter *Quality of Service* (QoS) yang terdiri dari *Packet Loss, Delay,* dan *Throughtput* pada 2 *client* yang terhubung ke router mikrotik dan setiap *client* akan menggunakan *protocol* yang berbeda. Semua *client* akan melakukan *video streaming* secara bersamaan untuk mendapatkan capture paket data. Hasil pengujian akan dikelompokkan menjadi empat kategori, yaitu kategori buruk, sedang, bagus dan sangat bagus. Diharapkan akan dihasilkan sebuah data yang dapat menunjukkan kualitas dari layanan kedua *protocol* tersebut. sehingga dapat dijadikan acuan dalam pemilihan *protocol* vpn yang akan digunakan [6].

Penelitian yang dilakukan oleh Dina Olvia dan Zulhendra pada tahun 2021 yang berjudul "Analisis *Quality of Service* (QoS) Jaringan *Virtual Private Network* (VPN) dengan menggunakan *protocol* IPSec (Studi Kasus : SMK Negeri 3 Pariaman)". Menurut peneliti kondisi jaringan komputer di Sekolah Menengah Kejuruan (SMK) Negeri 3 Pariaman memerlukan kualitas layanan jaringan yang primer agar kualitas pengiriman berjalan dengan baik, Informasi yang dilewatkan menggunakan *protocol* IPSec dapat memenuhi kondisi optimal sesuai parameter kualitas layanan QoS. Informasi yang akan dilewatkan dalam jaringan internet hendak dengan gampang dilihat oleh orang yang tidak bertanggung jawab bila tidak dipasangkan VPN, maka dari itu perlunya dipasangkan jaringan VPN di jaringan internet kepunyaan sekolah biar data yang dilalui lewat jaringan VPN akan cepat sampai serta terenkripsi dengan baik, Penerapan *protocol* IPSec yang merupakan salah satu bentuk VPN jenis L2TP, adalah kondisi *protocol* yang ingin dipantau

dalam penelitian ini berupa kualitas layanan jaringan sesuai parameter yang terdapat dalam QoS yang mana *delay, packet loss, throughput, jitter,* dan *bandwith*. Penelitian ini bertujuan untuk mengetahui, kualitas layanan jaringan VPN dengan memakai *protocol* IPSec di sekolah menengah kejuruan (SMK) Negeri 3 Pariaman, dengan parameter QoS untuk mengetahui besar hasil pengukuran dari perameter *delay, packet loss, throughput, jitter,* dan *bandwith.* Penelitian ini memakai tata cara kuantitatif dengan jenis penelitian deskriptif dengan menggunakan analisis statistik. Pengukuran *delay, packet loss, throughput, jitter,* dan *bandwith* menggunakan aplikasi axence nettols, hasilnya dibandingkan dengan standar TIPHON. Penelitian ini dilakukan selama tiga minggu dalam satu minggu enam hari pada saat pagi dan sore hari. Hasil analisis data menunjukkan: (1) kualitas layanan jaringan VPN Sekolah Menengah Kejuruan (SMK) Negeri 3 Pariaman termasuk kategori kualitas layanan yang berkualitas baik dibuktikan dengan hasil pengukuran parameter QoS memiliki nilai rata- rata memuaskan, (2) nilai pengukuran *delay* dengan standar TIPHON digolongkan sangat bagus dengan nilai rata – rata 34,7 ms pada pagi hari dan 32,9 ms pada sore hari, (3) nilai pengukuran throughput dengan standar TIPHON digolongkan bagus dengan nilai rata-rata 59% pada pagi hari dan 75% pada sore hari, (4) nilai pengukuran packet loss dengan standar TIPHON digolongkan sangat bagus dengan nilai rata-rata 2,5% pada pagi hari dan 1,6% pada sore hari, (5) nilai pengukuran jitter dengan standar TIPHON digolongkan sangat bagus dengan nilai rata-rata 0,007 ms pada pagi dan sore hari [7].

Penelitian yang dilakukan oleh Mardianto pada tahun 2019 yang berjudul *"Analisis Quality of Service (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3"*. Menurut peneliti internet yang terus menerus meningkat merupakan tantangan *Internet Service Provider* (ISP) untuk masa depan akan kebutuhan lalu lintas jaringan komputer global dan *Quality of Service* (QoS) yang diharapkan. Untuk menjaga agar kompetitif ISP di indonesia dengan perkembangan pemakaian internet menyebabkan permintaan QoS harus ditingkatkan. Jaringan MPLS VPN menggabungkan teknologi *switching layer* 2 dengan teknologi *routing l*ayer 3. Jaringan MPLS VPN muncul sebagai teknologi yang memenuhi persyaratan VPN seperti *private IP*, dan kemampuan untuk

mendukung alamat yang bertumpuk dalam menyelesaikan masalah kecepatan dan QoS. Metode yang digunakan adalah riset ekperimental. Dari hasil pengukuran diperoleh *delay* jaringan VPN dan MPLS VPN memilik nilai *delay* sangat bagus. Untuk *throughput* pada jaringan VPN memiliki kualitas sedang dan pada jaringan MPLS VPN memiliki kualitas Bagus. Dan untuk nilai *packet loss* untuk kedua jenis jaringan adalah 0 %. Hal ini menunjukan bahwa throughput jaringan MPLS VPN memiliki QoS yang lebih Bagus sedangkan untuk *delay* dan *packet loss* pada jaringan VPN dan MPLS VPN memiliki nilai kualitas yang sama [8].

Penelitian yang dilakukan oleh Moezes Rasuanda dan Haeruddin pada tahun 2020 yang berjudul *"Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode Quality of Service"*. Menurut peneliti dengan majunya perkembangan teknologi begitu juga dengan keamanannya yang sudah seharusnya ditingkatkan. Maka dari itu banyak cara untuk para pengguna meningkatkan keamanan jaringan internet mereka sendiri, dikarenakan tingkat keamanan dari sebuah jaringan sangat lah penting untuk pengguna terhadap data-data yang melintas di jaringan tersebut, seperti perbankan, perusahaan besar, instansi pemerintah dan banyak lagi pengguna yang sangat membutuhkan keamanan jaringan mereka karena segala proses transaksi serta proses kerja berlangsung secara online sehingga menjadi titik tumpu penting nya sebuah keamanan jaringan tersebut. Banyak cara untuk mengamankan sebuah jaringan salah satunya adalah menggunakan VPN, salah satu cara yang mudah dan paling banyak digunakan oleh pengguna untuk mengamankan jaringan mereka, dan tidak hanya satu jenis namun VPN mempunyai banyak jenis atau bisa dibilang *protocol*, diantara lainnya ada PPTP, L2TP, IPSec, IKEv2, MPLS, SSTP, SSL-VPN. Dan Tujuan dari penelitian ini adalah untuk menguji serta membandingkan performa dari kedua *protocol* VPN yang sudah ditentukan yaitu *protocol* PPTP dan SSL, dengan menggunakan metode *Quality of Service* yang dimana metode ini adalah cara untuk mengukur seberapa baiknya jaringan tersebut dan juga memastikan pengguna mendapatkan qualitas dari servis yang terbaik [9].

Tabel 2.1 Tabel penelitian sebelumnya

No	Jurnal	Tujuan Penelitian	Kesimpulan	Saran atau kelemahan	Perbandingan
1	Analisis *Quality of Service* (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3 (Mardianto, 2019)	Adanya perbedaan prinsip kerja dari jaringan VPN dan MPLS VPN maka terdapat perbedaan dari segi QoS yang diberikan sehingga perlu dilakukan analisis terhadap QoS pada kedua jenis jaringan yang ditawarkan oleh ISP.	1. jaringan VPN dan MPLS VPN memilik nilai *delay* sangat bagus. Akan tetapi pada jaringan MPLS VPN dapat memperpendek proses *routing* dalam pengirimanpaket sehingga paket data akan cepat sampai ke tujuan dibandingkan dengan jaringan VPN. 2. MPLS VPN memiliki throughput yang stabil sehingga jaringan MPLS VPN dapat mendukung QoS lebih baik dibandingkan dengan jaringan VPN.	Sebaiknya bandingkan lagi jenis *protocol* VPN lainnya, karena jenis *protocol* VPN tidak hanya *protocol* L2TP saja.	Pada penelitian sebelumnya membandingkan antara VPN dengan MPLS VPN. Objek pengujian menggunakan FTP dalam melakukan pengiriman data. Pada penelitian sekarang membandingkan antara jenis VPN PPTP, L2TP, dan OpenVPN. Objek pengujian menggunakan autopilot sebagai pengiriman data.

No	Jurnal	Tujuan Penelitian	Kesimpulan	Saran atau kelemahan	Perbandingan
			3. Dalam hal *packet loss* pada jaringan VPN dan MPLS VPN 0 % dengan demikian kualitas layanan sangat bagus. hal ini diakibatkan apabila terjadi kehilangan paket penerima akan meminta retransmission atau pengiriman secara otomatis *resends* sehingga tidak diperoleh kehilangan paket.		
2	Analisa Perbandingan *Quality Of Service* Antara *Protocol* PPTP dan L2TP Pada *Virtual Private Network* Berbasis Router Mikrotik (Dahnial, 2019)	Untuk mengetahui *protocol* manakah yang menghasilkan performa terbaik pada jaringan VPN.	1. Masing – masing parameter pada setiap percobaan menunjukkan kualitas yang sama. Tetapi perbedaan terdapat pada nilai masing – masing parameter QoS. 2. Kinerja *protocol* PPTP pada jaringan VPN lebih	Kelemahan dari penelitian tersebut adalah tidak dijelaskan mengenai objek apa yang digunakan sebagai pengujian pengiriman dan penerimaan data, sehingga menimbulkan ambigu apakah	Pada penelitian sebelumnya menggunakan *protocol* VPN jenis PPTP dan L2TP. Pada penelitian sekarang menggunakan *protocol* VPN PPTP, L2TP, dan OpenVPN.

No	Jurnal	Tujuan Penelitian	Kesimpulan	Saran atau kelemahan	Perbandingan
			baik dari *protocol* L2TP dari pengujian sisi *Quality of Service* (QoS) yang dilakukan.	pengujian dilakukan hanya sebatas pengiriman paket ICMP atau pengujian lainnya.	
3	Analisis Perbandingan Kinerja Jaringan *Secure Socket Tunneling Protocol* (Sstp) Dan *Layer Two Tunneling Protocol* (L2tp) + *Internet Protocol Security* (Ipsec) Menggunakan Metode *Quality Of Service* (Qos) (Lukman, Aiman Mukhlishah, 2020)	Untuk mengetahui metode tunneling VPN mana yang terbaik antara SSTP dengan L2TP + IPSec.	Hasil penelitian bisa diambil kesimpulan bahwa L2TP+IPSec lebih baik dibanding SSTP, dinilai dari parameter QOS yang sudah diuji dan dibandingkan.	Kelemahan dalam penelitian tersebut adalah tidak dijelaskan mengenai tempat yang digunakan untuk pengujian, apakah pengujian dilakukan menggunakan aplikasi simulasi atau pengujian dilakukan dengan menguji kualitas jaringan sebuah perusahaan.	Pada penelitian sebelumnya menggunakan VPN jenis SSTP dan L2TP+IPsec. Melakukan pengujian dengan cara memutar youtube dan mendownload vidio, menggunakan *protocol* TCP. Pada penelitian sekarang menggunakan VPN PPTP, L2TP, dan OpenVPN. Menggunakan objek autopilot sebagai pengujiannya.Menggunakan *protocol* UDP.

No	Jurnal	Tujuan Penelitian	Kesimpulan	Saran atau kelemahan	Perbandingan
4	Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode *Quality of Service. (*Moezez Rasuandra, Haeruddin, 2020)	Untuk menguji serta membandingkan performa dari kedua *protocol* VPN yang sudah ditentukan yaitu *protocol* PPTP dan SSL, dengan menggunakan metode *Quality of Service.*	1. VPN PPTP memiliki kelebihan dimana mendukung semua sistem operasi desktop dan seluler, setup konfigurasi sederhana, dan memiliki kecepatan yang baik. Dan memiliki kekurangan dimana mudah untuk diblokir oleh ISP, tingkat enkripsi tidak begitu tinggi. 2. VPN SSTP memiliki kelebihan dimana mampu menembus *firewall*, dan terdukung penuh oleh sistem operasi Windows. Sedangkan kekurangan dari VPN ini ialah tidak bisa melakukan backdoor, dan sementara masih	Kelemahan dalam penelitian tersebut adalah antara judul dengan isi pembahasan tidak cocok, dimana dalam judul pengujian VPN menggunakan metode QoS, namun dalam pembahasan sama sekali tidak menjelaskan mengenai parameter yang digunakan serta hasi nilai QoS yang diperoleh dari pengujian tersebut.	Pada penelitian sebelumnya menggunakan VPN jenis PPTP dan SSTP. Pada penelitian sekarang menggunakan VPN jenis PPTP, L2TP, dan OpenVPN.

No	Jurnal	Tujuan Penelitian	Kesimpulan	Saran atau kelemahan	Perbandingan
			terfungsi hanya pada platform Windows.		
5	Analisis *Quality of Service* (QoS) Jaringan Virtual Private Network (VPN) dengan menggunakan *protocol* IPSec (Studi Kasus : SMK Negeri 3 Pariaman) (Dina Olvia, Zulhendra, 2021)	Untuk mengetahui kualitas layanan jaringan VPN di SMK Negeri 3 Pariaman.	Kualitas layanan jaringan VPN di SMK Negeri 3 Pariaman termasuk kedalam kategori jaringan yang berkualitas baik dibuktikan dengan hasil pengukuran penelitian yang memiliki nilai rata-rata memuaskan menggunakan parameter QoS *delay*, packet loss, throughput, jitter, dan bandwith yang mana jaringan VPN di SMK Negeri 3 Pariaman memiliki kualitas yang memuaskan.	Saran untuk penelitian sebelumnya pada saat melakukan pengujian dilakukan juga pada saat saat tidak ada aktifitas yang menggunakan jaringan tersebut, sehingga nanti hasil komparasi lebih maksimal antara pada saat jam sibuk dan pada saat jam senggang.	Pada penelitian sebelumnya hanya menggunakan VPN L2TP. Studi kasus di SMK Negeri 3 Pariaman. Pada penelitian sekarang menggunakan VPN jenis PPTP, L2TP, dan OpenVPN. Studi kasus di Pustekbang-BRIN.

2.2. Landasan Teori

Beberapa dasar teori terkait yang digunakan dalam penelitian ini:

2.2.1. Pengertian Jaringan Komputer

Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling berhubungan satu sama lain untuk melakukan komunikasi data dengan menggunakan *protocol* komunikasi melalui media komunikasi (kabel atau nirkabel), sehingga komputer - komputer tersebut dapat saling berbagi informasi, data, program - program, dan penggunaan perangkat keras secara bersama. Dalam hal ini komunikasi data yang bisa dilakukan melalui jaringan komputer dapat berupa teks, gambar, video, dan suara [10].

Manfaat Jaringan Komputer secara umum yang akan bisa didapatkan adalah sebagai berikut [11]:

1. Jaringan Komputer mendapatkan *sharing resource* (data, program, peripheral komputer)
2. Jaringan Komputer media komunikasi efektif dan multimedia
3. Jaringan Komputer memungkinkan manajemen sumber daya lebih efisien.
4. Jaringan Komputer memungkinkan penyampaian lebih terpadu.
5. Jaringan Komputer memungkinkan kelompok kerja berkomunikasi lebih efisien.
6. Jaringan Komputer dapat menjaga keamanan data lebih terjamin (hak akses).
7. Jaringan Komputer menghemat biaya pengembangan dan pemeliharaan.
8. Jaringan Komputer membantu mempertahankan informasi agar tetap handal dan *up to date*.

2.2.2. *Internet Protocol* (IP)

Internet protocol (IP) merupakan *protocol* yang paling penting yang harus berada pada layer Internet TCP/IP. Semua *protocol* TCP/IP yang berasal dari layer

mengirmkan data melalui *protocol* IP ini. Seluruh data dilewatkan, dioalah oleh *protocol* IP dan dikirimkan sebagai datagram IP untuk sampai ke sisi penerima. Dalam melakukan pengiriman data, *protocol* IP ini bersifat *unrealible connectionless*, dan *datagram delivery service.*

Iinternet proctocol address (IP Address) merupakan deretan angka biner antara 32 bit sampai dengan 128 bit yang digunakan sebagai alamat identifikasi untuk tiap komputer host dalam jaringan internet. Angka 32 bit digunakan untuk alamat *IP Address* versi IPv4 dan angka 128 bit digunakan untuk menunjukkan alamat dari komputer pada jaringan internet berbasis TCP/IP [12].

1. *Internet Protocol Version* 4 (IPv4)

   Internet proctocol version 4 atau Ipv4 terdiri dari 32-bit dan bisa menampung lebih dari 4.294.967.296 host di seluruh dunia. Sebagai contoh yaitu 172.146.80.100, jika host diseluruh dunia melebihi angka 4.294.967.296 maka dibuatlah Ipv6 [12].

2. *Internet Protocol Version 6* (IPv6)

   IPv6 diciptakan untuk menjawab kekhawatiran akan kemampuan Ipv4 yang hanya menggunakan 32 bit untuk menampung *IP Address* di seluruh dunia, semakin banyaknya pengguna jaringan internet dari hari ke hari di seluruh dunia Ipv4 dinilai suatu saat akan mencapai batas maksimum yang dapat ditampungnya.

   Internet protocol versi 6 atau Ipv6 ini terdiri dari 128 bit. IP ini 4 kali dari Ipv4, tetapi jumlah host yang bisa ditampung bukan 4 kali dari 4.294.967.296 melainkan 4.294.967.296 pangkat4, jadi total 340.282.366.920.938.463.463.374.607.431.768.211.456 [12].

2.2.3. *User Datagram Protocol* (UDP)

Protocol ini untuk mendukung konsep jaringan berbasis IP. Telah diketahui bahwa IP *(internet protocol*) sebagai *protocol* jaringan internet yang mengkomunikasikan dua titik jaringan serta secara spesifik semua aplikasi dan

layanan terpengaruh port tetapi kondisi konsep jaringan IP tidak memberikan jaminan. Jaminan tersebut adalah jaminan bahwa data akan tersampaikan pada destination yang benar dan data tersampaikan dengan benar [13].

Berbeda dengan TCP, *protocol* UDP adalah *protocol* yang bersifat *connectionless* dalam mentransmisi data dan tidak mengenal dalam pengecekan terhadap error pengiriman data. *Protocol* UDP pada dasarnya hanya mengandung IP dengan tambahan header singkat. *Protocol* UDP tidak melakukan sebuah proses kontrol alur data, kontrol kesalahan ataupun pengiriman ulang terhadap kesalahan sehingga hanya menyediakan interface ke *protocol* IP. UDP sangat berguna sekali pada situasi *client server* dan penjelasan UDP lebih detail dapat ditemui pada RFC 768. UDP memiliki karaketeristik yaitu sebagai berikut [13]:

1. *End-to-end*, UDP dapat mengidentifikasi proses yang berjalan dalam komputer.
2. *Connectionless*, UDP memiliki paradigma Connectionless tanpa membuat koneksi sebelumnya dengan tanpa adanya kontrol.
3. *Message-oriented*, mengirimkan dan menerima data secara segmen.
4. *Best-effort*, yang utama adalah pengiriman yang terbaik.
5. *Arbitrary interaction*, UDP dapat menerima dan mengirim dari banyak proses.
6. *Operating system independent*, berdiri sendiri dalam *operating system.*

2.2.4. Routing Protocol

Routing protocol adalah aturan atau cara pencarian jalur terbaik yang digunakan untuk mengirimkan paket data dari *node* pengirim ke *node* penerima. Paket akan melewati beberapa *node* penghubung, dimana *protocol routing* berfungsi untuk mencarikan jalur yang terbaik dari beberapa jalur yang akan dilalui melalui mekanisme pembentukan tabel *routing* [14]. *Protocol routing* sangat dibutuhkan untuk mengirimkan sebuah paket data dari *node* pengirim ke *node* penerima, dengan melewati beberapa *node* penghubung (intermediate *node*), dimana *protocol routing* bertugas untuk mencari rute terbaik dari link yang akan

dilalui. Pemilihan rute terbaik tersebut dipilih berdasarkan beberapa pertimbangan seperti bandwith link dan jaraknya. Selain itu, *protocol routing* juga bertugas untuk mengatur cara komunikasi dua *node* selama pertukaran informasi. Hal ini termasuk prosedur dalam membangun rute, keputusan dalam forwarding dan tindakan dalam menjaga rute atau memperbaiki *routing* yang gagal [15].

Routing protocol dibagi menjadi 2 berdasarkan karakteristiknya, yaitu:

1. *Routing Statis*

   Routing Statis adalah *routing protocol* yang memilih rute pengiriman hanya berdasarkan rute yang telah ditentukan pada table *routing* dan hanya bisa dirubah secara manual oleh *Network Adminstrator*. Kelebihan dari *routing statis* jika dibandingkan dengan *routing* dinamis adalah proses *routing* lebih mudah dikenali dengan alamat network IP yang sudah pasti [16].

2. *Routing Dinamis*

   Routing dinamis adalah *routing* yang memilih rute pengiriman data berdasarkan kondisi yang ada di jaringan tersebut. Kelebihan dari *dynamic routing* jika dibandingkan dengan *static routing* adalah proses tabel *routing* lebih mudah tanpa adanya input dari operator atau admin jaringan [16].

   Routing dinamis sendiri terbagi menjadi 2 berdasarkan *environment*-nya, yaitu: *Interior Gateway Protocol* dan *Exterior Gateway Protocol. Interior Gateway Protocol* bekerja di dalam *Autonomous System,* sedangkan *Exterior Gateway Protocol* bekerja diantara *Autonomous System*. Contoh dari *Routing protocol* adalah [14]:

   a. *Routing Information Protocol* (RIP)
   b. *Interior Gateway Routing Protocol* (IGRP)
   c. *Enhanced Interior Gateway Routing Protocol* (EIGRP)
   d. *Open Shortest Path Firs* (OSPF)
   e. *Intermediate System-to-Intermediate System* (IS-IS)
   f. *Border Gateway Protocol* (BGP)

2.2.5. *Virtual Private Network* (VPN)

Virtual Private Network (VPN) adalah teknik pengaman jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet [17].

Menurut Athailah untuk membuat sebuah VPN, diperlukan sebuah *protocol* sehingga dapat berjalan dengan baik bagaikan koneksi point-to-point sesungguhnya. Saat ini tersedia banyak sekali *protocol* VPN yang dapat digunakan [10].

1. *Point-to-Point Tunneling Protocol* (PPTP)

   Point to Point Tunneling Protocol (PPTP) merupakan *protocol* jaringan yang memungkinkan pengamanan transfer data dari remote *client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access point-to-point protocol* (PPP) yang dikeluarkan *Internet Engineering Task Force* (IETE).

   Biasanya PPTP ini digunakan untuk jaringan yang sudah melewati *multihop router (Routed Network*). Jika anda ingin menggunakan PPTP pastikan di Router anda tidak ada rule yang melakukan *blocking* terhadap *protocol* TCP port 1723 dan *IP Protocol* 47/GRE karena *service* PPTP menggunakan *protocol* tersebut [10].

2. *Layer 2 Transfer Protocol* (L2TP)

   Layer 2 Transfer Protocol (L2TP) adalah pengembangan dari PPTP *plus* L2F. *Protocol Tunneling Layer 2* (L2TP) juga sering disebut sebagai protocol dial-up virtual, karena L2TP memperluas sesi *dial-up Point to Point Protocol* (PPP) melalui jaringan internet public dan memiliki tingkat keamanan yang lebih tinggi dibandingkan PPTP yang hanya menggunakan MPPE.

   IPSec merupakan *protocol* yang digunakan untuk mengamankan transmisi datagram pada jaringan berbasis TCP/IP. IPSec menawarkan 3

layanan utama, yaitu otentikasi dan integritas data, kerahasiaan, dan manajemen kunci. Untuk dapat memenuhi kebutuhan keamanan L2TP perlu dicoba implementasi keamanan dengan menggunakan *protocol* tipe *transport IPSec* atau lebih dikenal dengan *protocol* L2TP *over IP Security* (IPSec), sehingga paket informasi yang dikirim oleh *protocol* L2TP akan terenkapsulasi oleh *protocol* IPSec [18].

3. OpenVPN

OpenVPN merupakan aplikasi *open source* untuk membuat *Virtual Private Network* (VPN), aplikasi ini dapat membangun koneksi *point-to-point tunnel* yang terenkripsi dengan menggunakan kombinasi *keys, certificate*, atau *username-password*, kombinasi enkripsi tersebut diperlukan pada proses otentikasi berlangsung [19].

2.2.6. Quality of Service (QoS)

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis[20]. Terdapat 3 tingkatan QoS yang sering digunakan yaitu *Best-effort service, Integrated service*, dan *Differentiated service* [21].

1. *Best-effort service* yaitu sebuah model *service* yang mana sebuah aplikasi pada setiap kali mengirimkan data diharuskan tanpa harus meminta izin kepada jaringan komputer.
2. *Integrated service* yaitu sebuah *service* yang berfungsi serta dapat menampung beberapa persyaratan dari QoS. Dalam *service* ini sebuah aplikasi meminta jenis service tertentu dahulu sebelum mengirimkan data dan aplikasi ini diharapkan dapat mengirimkan datanya hanya setelah mendapat konfirmasi terlebih dahulu dari jaringan.
3. *Differentiated service* yaitu sebuah *service* yang dapat memenuhi persyaratan dari QoS yang berbeda, tapi tidak seperti pada *Integrated service* pada jenis ini tidak secara eksplisit memberi isyarat router sebelum mengirimkan datanya.

Adapun ketentuan parameter QoS berdasarkan Standard TIPHON yang dipergunakan untuk membandingkan hasil QoS yang dihasilkan berdasarkan pengamatan paramater *delay*, *jitter*, *packet loss* dan *throuhput* [22].

1. *Delay*

Delay (Latency) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, congesti atau juga waktu proses yang lama [22].

Persamaan untuk menghitung *delay* adalah:

$$Delay\ rata\ rata = \frac{Total\ delay}{Total\ paket\ yang\ diterima} \quad [2.1]$$

Tabel 2.2 Kategori *Delay*

Kategori *Delay*	**Besar *Delay***	**Indeks**
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	301 s/d 450 ms	2
Buruk	> 450 ms	1

Sumber : ETSI 1999-2006 [23]

2. *Jitter*

Jitter merupakan variasi kedatangan paket data. Hal tersebut diakibatkan oleh variasi panjang antrian, waktu pengolahan data, dan waktu penghimpunan ulang paket di akhir perjalanan *Jitter* [22].

Persamaan untuk menghitung *jitter* adalah:

$$Jitter = \frac{Total\ variasi\ delay}{Total\ paket\ yang\ diterima} \quad [2.2]$$

Total variasi *delay* dipeoleh dari:

$$Total\ Variasi\ Delay = Delay - (Rata - rata\ Delay) \quad [2.3]$$

Tabel 2.3 Kategori *Jitter*

Kategori Jitter	Peak Jitter	Indeks
Sangat Bagus	0 ms	4
Bagus	1 s/d 75 ms	3
Sedang	76 s/d 225 ms	2
Buruk	> 225 ms	1

Sumber: ETSI 1999-2006 [23]

3. 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 [22].

Persamaan untuk menghitung *packet loss* adalah:

$$Packet\ Loss = \frac{Paket\ dikirim - paket\ diterima}{paket\ yang\ diterima}\ x\ 100\% \qquad [2.4]$$

Tabel 2.4 Kategori *Packet Loss*

Kategori Packet Loss	Packet Loss	Indeks
Sangat Bagus	*0% - 2%*	*4*
Bagus	*3% - 14%*	*3*
Sedang	*15% - 24%*	*2*
Buruk	*> 25 %*	*1*

Sumber : ETSI 1999-2006 [23]

2.2.7. Mikrotik Router OS

Mikrotik adalah perangkat jaringan komputer yang berupa *hardware* dan *hoftware* yang dapat difungsikan sebagai Router, sebagai alat *filtering*, *switching* maupun yang lainnya. Adapun *hardware* Mikrotik bisa berupa Router PC (yang diinstall pada PC) maupun berupa Router Board (sudah dibangun langsung dari perusahaan Mikrotik)[24]. Sedangkan *software* Mikrotik Adalah versi Mikrotik dalam bentuk perangkat lunak yang dapat diinstal pada komputer rumahan (PC) melalui CD. File image MikroTik RouterOS dapat diunduh dari website resmi Mikrotik [25].

Mikrotik dikenal dengan istilah level pada lisensinya, mulai level 0 kemudian 1, 3, hingga 6. Setiap level memiliki kemampuan yang berbeda sesuai harganya. Penjelasan setiap level mikrotik sebagai berikut:

1. Level 0 (gratis). Level ini tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
2. Level 1 (demo). Pada level ini user dapat menggunakannya sebagai *routing* standar dengan 1 pengaturan, dan tidak memiliki limitasi waktu untuk menggunakannya.
3. Level 3. Level ini mencakup level 1 ditambah dengan kemampuan untuk memanajemen *hardware* berbasis kartu jaringan atau Ethernet dan pengelolan perangkat *wireless* tipe *client*.
4. Level 4. Level ini mencakup level 1 dan 3 ditambah kemampuan untuk mengelola perangkat *wireless* tipe *access point*.
5. Level 5. Level ini mencakup level 1, 3, dan 4 ditambah kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
6. Level 6. Level ini mencakup semua Level dan tidak memiliki limitasi atau batasan apapun.

2.2.8. Graphic Network Simulator Version 3 (GNS3)

Graphic Network Simulator Version 3 (GNS3) adalah sebuah program *graphical network simulator* yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan simulator lainnya. Program ini dapat dijalankan di berbagai sistem operasi, seperti Windows, Linux, atau MacOS X. Fitur-fitur yang didukung GNS3 antara lain [26]:

1. Fitur-fitur yang didukung GNS3 antara lain:
2. Mengemulasikan berbagai platform Cisco IOS router, IPS, PIX dan ASA *firewall*, JUNOS.
3. Simulasi Ethernet sederhana, ATM dan *Frame Relay switch*.

4. Koneksi antara jaringan simulasi dengan jaringan yang sesungguhnya di dunia nyata.
5. Dapat dihubungkan ke jaringan fisik.
6. Dapat diintegrasikan dengan Wireshark *(tools packet capture/analyzer)* untuk analisa *traffic* jaringan.

2.2.9. Wireshark

Wireshark adalah salah satu analisis paket bebas serta sumber terbuka. Perangkat ini untuk digunakan sebagai pemecah suatu permasalahan jaringan, analisis, perangkat lunak dan serta mengembangkan *protocol* komunikasi, dan juga pendidikan, dari sekian banyak aplikasi *Network Analyzer* yang banyak digunakan oleh *Network Administrator* untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang di kelola Wireshark. Wireshark mampu menangkap paket-paket data yang ada pada jaringan tersebut. Semua jenis paket informasi dalam berbagai format *protocol* pun akan dengan mudah ditangkap dan dianalisa [27].

Ada beberapa fitur Wireshark:

1. Berjalan pada sistem operasi Linux dan Windows
2. Menangkap paket *(Capturing Packet)* langsung dari *network interface*
3. Mampu menampilkan hasil tangkapan dengan detail
4. Dapat melakukan pem*filter*an paket.
5. Hasil tangkapan dapat di *save*, di *import* dan di *export*

2.2.10. *Hardware In The Loop Simulations* (HILS)

Perancangan simulasi dibagi menjadi dua tipe metode, yaitu *Model in The Loop* (MIL) dan *Hardware in The Loop* (HIL). MIL adalah langkah awal dari model *design controller*. MIL merupakan tingkat integrasi pertama dan didasarkan pada model sistem itu sendiri. MIL juga mengesankan respon global sehubungan dengan stabilitas dan penyesuaian model yang diinginkan. Pengujian *Model in The Loop* merupakan metode dimana objek uji dibagi menjadi dua bagian yaitu, bagian fisik

dan bagian simulasi. Dan bagian ini terhubung membentuk gabungan fisik *numeric* [28].

HIL adalah teknik pengujian dinamis yang mensimulasikan *input/output* perilaku dari sistem fisik yang di *interface* ke sistem kontrol. Pengujian HIL memungkinkan *desainer* untuk mensimulasikan perilaku *real-time* dan karakteristik dari sistem, sehingga untuk menguji perangkat *Device Under Test* (DUT) yang beroperasi pada sistem fisik, tanpa perlu perangkat keras yang sebenarnya atau lingkungan operasional. HIL berguna untuk validasi skema koordinasi perlindungan di antara perangkat perlindungan tegangan rendah. Sistem HIL dapat meningkatkan kecepatan pengujian [28].