USULAN TUGAS AKHIR

ANALISIS PERBANDINGAN KINERJA TCP DAN UDP PADA JARINGAN MPLS DAN NON-MPLS DENGAN TUNNELING L2TP/IPSEC BERDASARKAN PROTOKOL ROUTING OSPF, RIPv2 DAN BGP

Oleh :

BAIQ ALUNG SEPTIYA NIRMALA

F1D 016 014

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MATARAM

2020

Usulan Tugas Akhir

Analisis Perbandingan Kinerja TCP dan UDP Pada Jaringan MPLS dan Non-MPLS dengan *Tunneling* L2TP/IPSec Berdasarkan Protokol *Routing* OSPF, RIPv2 dan BGP

Oleh:

Baiq Alung Septiya Nirmala

F1D016014

Telah diperiksa oleh Tim Pembimbing

1. Pembimbing I,

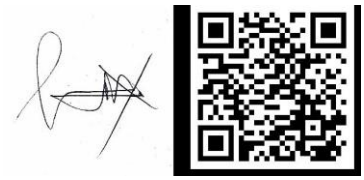
Andy Hidayat Jatmika, S.T., M.Kom. Tanggal: 23 Juni 2020
Nip. 19831209 201212 1 001

2. Pembimbing II,

Ariyan Zubaidi, S.Kom., M.T. Tanggal: 23 Juni 2020
Nip. 19860913 201504 1 001

Telah disetujui oleh Tim Penguji

1. Penguji I,



Dr.Eng. I Gde Putu Wirarama Wedashwara Wirawan, S.T.,M.T.
Nip. 19840919 201803 1 001

Tanggal: 23 Juni 2020

2. Pengujii II,

Ahmad Zafrullah Mardiansyah, S.T., M.Eng.
Nip.

Tanggal: 23 Juni 2020

3. Penguji III,

Arik Aranta, S.Kom., M.Kom.
Nip. 199402202019031004

Tanggal: 23 Juni 2020

Mengetahui,
Ketua Program Studi Teknik Informatika
Fakultas Teknik
Universitas Mataram

Prof. Dr. Eng. I Gede Pasek Suta Wijaya, S.T., M.T.
19731130 200003 1 001

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Aktivitas pertukaran data yang semakin padat pada jaringan internet tentunya memerlukan kecepatan pada saat transfer data, keakuratan data yang sampai pada penerima dan keamanan data pada saat proses transfer data. Sehingga pengembangan teknologi jaringan menjadi hal penting untuk diteliti. Protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) pada *layer transport* yang berperan dalam proses transfer data. TCP memiliki kelebihan yaitu dapat memastikan keakuratan data yang sampai ke penerima. Sedangkan UDP memiliki keunggulan dalam hal kecepatan transfer data. Penerapan kedua protokol tersebut dapat disesuaikan dengan kebutuhan. Oleh karena itu, kinerja dari TCP dan UDP perlu dilakukan analisis dan perbandingan terhadap suatu kondisi tertentu seperti penerapannya pada suatu teknologi yang dapat meningkatkan kinerja jaringan. Pada penelitian ini *Quality of Service* (QoS) dari TCP dan UDP akan dibandingkan pada jaringan *Multiprotocol Label Switching* (MPLS) yang dikombinasikan dengan *tunneling Layer 2 Tunneling Protocol / Internet Protocol Security* (L2TP/IPSec). Kinerja TCP dan UDP dibandingkan berdasarkan beberapa protokol *routing* yaitu *Open Shortest Path First* (OSPF), *Routing Information Protocol version 2* (RIPv2) dan *Border Gateway Protocol* (BGP). Tujuan dari penelitian ini yaitu untuk mengetahui perbandingan QoS dari TCP dan UDP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* OSPF, RIPv2 dan BGP untuk dapat memberikan referensi dalam memilih teknologi yang sesuai dengan kebutuhan. Penelitian ini akan dilakukan dengan menggunakan simulator *Graphical Network Simulator-3* (GNS3) dan *tools* Iperf v.3.6 untuk mengukur nilai QoS dari TCP dan UDP.

Kata Kunci : Jaringan Internet, TCP, UDP, MPLS, L2TP/IPSec, Protokol *Routing*, OSPF, RIPv2, BGP, GNS3.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini hampir semua kegiatan dan aktivitas dalam berbagai bidang dilakukan dengan memanfaatkan jaringan internet. Aktivitas pertukaran data yang semakin padat tentunya bukan hanya memerlukan kecepatan pada saat transfer data saja, tetapi juga keakuratan data yang sampai pada penerima dan keamanan data pada saat proses transfer data. Meningkatnya kebutuhan akan penggunaan jaringan internet dan juga penggunanya tentunya perlu juga adanya peningkatan efektifitas teknologi pada jaringan internet dalam hal kecepetan pengiriman data, keakuratan data hingga keamanan data. Oleh karena itu, perlu adanya suatu pengembangan teknologi pada jaringan internet untuk mendukung aktivitas para pengguna jaringan internet, salah satunya dengan memanfaatkan protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) dimana penggunaannya dapat disesuaikan dengan kebutuhan setiap pengguna apakah lebih mementingkan kecepatan transfer data atau keakuratan data.

TCP dan UDP merupakan protokol pada *Layer Transport*. Pada saat transfer data melalui jaringan jika dilihat dari *Open Systems Interconnection* (OSI) *layer*, *layer* yang berfungsi untuk menangani proses transfer data yaitu *Layer Transport*. Pada *layer transport* terdapat dua protokol utama yang paling sering digunakan yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). TCP memiliki kemampuan untuk memastikan setiap data yang dikirimkan akan sampai secara utuh ke penerima, sehingga tidak perlu khawatir data yang dikirimkan tidak sampai ke penerima secara utuh. Sedangkan UDP memilki kemampuan dalam kecepatan pengiriman data dan lebih unggul dari TCP dalam hal kecepatan.

Jaringan *Multiprotocol Label Switching* (MPLS) merupakan salah satu solusi yang dapat digunakan untuk meningkatkan performa suatu jaringan dengan meningkatkan *Quality of Service* (QoS). MPLS merupakan teknologi yang dapat memberikan alternatif dalam proses pengiriman paket pada jaringan. Pada jaringan MPLS tersebut juga dapat ditambahkan *tunneling* L2TP/IPSec yang akan mengamankan saluran komunikasi dan akan mengenkripsi data yang akan

dikirim. L2TP/IPSec merupakan gabungan dari L2TP (*Layer* 2 *Transfer Protocol*) dan IPSec (IP *Security*) dimana penggabungan dari dua teknologi *tunneling* ini bertujuan agar *tunneling* yang dilakukan dapat lebih baik.

Untuk membandingkan kinerja TCP dan UDP pada jaringan MPLS dengan *tunneling* L2TP/IPSec, dapat dilihat kinerjanya pada protokol *routing* yang berbeda-beda. Pada penelitian ini digunakan protokol *routing Open Shortest Path First* (OSPF), *Routing Information Protocol Version* 2 (RIPv2) dan *Border Gateway Protocol* (BGP). OSPF merupakan protokol *routing* berjenis *link state* yang memiliki kelebihan yaitu tidak ada batasan jumlah hop, serta memiliki konvergensi yang cepat. OSPF memiliki skalabilitas lebih baik dibandingkan protokol lainnya yang menggunakan *distance vector*. RIPv2 merupakan protokol *routing* berjenis *distance vector* yang mencari hop terpendek untuk mencapai tujuan. Jika kecepatan *link* sama, maka RIPv2 dapat bekerja lebih baik dibandingkan OSPF. BGP merupakan protokol berjenis *distance vector* yang biasanya digunakan oleh perusahaan penyedia layanan ISP. BGP memiliki kemampuan yang sangat handal dengan melakukan pengumpulan rute, pertukaran rute dan menetukan jalur terbaik untuk mencapai tujuan.

Pada penelitian ini akan dilakukan analisis dan juga pembandingan *Quality of Service* (QoS) TCP dan UDP pada jaringan MPLS menggunakan *tunneling* L2TP/IPSec dengan jaringan MPLS tanpa menggunakan *tunneling* dan pada jaringan Non-MPLS berdasarkan protokol *routing* yang digunakan yaitu OSPF, RIPv2 dan BGP. Parameter *Quality of Service* yang digunakan yaitu *throughput*, *jitter* dan *delay* yang akan diukur dengan *tool* Iperf. Simulasi akan dilakukan dengan menggunakan simulator *Graphic Network Simulator version 3* (GNS3) dan Wireshark sebagai *network analyzer*. Hasil dari penelitian ini diharapkan dapat menjadi perbandingan dengan penelitian sebelumnya dan juga acuan untuk penelitian selanjutnya yang berkaitan dengan TCP dan UDP ataupun jaringan MPLS dan *tunneling* L2TP/IPSec. Dari penelitian ini juga diharapkan dapat menambah referensi bagi para *Network Administrator* untuk memilih jenis jaringan internet yang lebih efisien.

1.2 Rumusan Masalah

Berdasarkan latar belakang, didapatkan rumusan masalah yaitu Bagaimana perbandingan *Quality of Service* (*Throughput*, *Delay*, dan *Jitter*) dari TCP dan UDP pada jaringan MPLS dan Non-MPLS menggunakan *tunneling* L2TP/IPSec berdasarkan protokol *routing* OSPF, RIPv2 dan BGP?

1.3 Batasan Masalah

Untuk mempersempit cakupan masalah tugas akhir ini agar tidak menyimpang dan lebih terarah, diberikan batasan masalah sebagai berikut :

1. Penelitian dilakukan untuk membandingkan *Quality of Service* (*Throughput*, *Delay*, dan *Jitter*) dari TCP dan UDP pada jaringan MPLS dan Non-MPLS dengan *tunneling* L2TP/IPSec.
2. Penelitian ini dilakukan berdasarkan protokol *routing* OSPF, RIPv2 dan BGP.
3. Penelitian dilakukan dengan menggunakan simulator *Graphic Network Simulator version 3* (GNS3).
4. Penelitian ini dilakukan menggunakan IPv4.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengetahui perbandingan *Quality of Service* (*Throughput*, *Delay*, dan *Jitter*) protokol TCP dan UDP pada jaringan MPLS dan Non-MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* OSPF, RIPv2 dan BGP.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini yaitu sebagai berikut :

1. Dapat mengetahui *Quality of Service Quality of Service* (*Throughput*, *Delay*, dan *Jitter*) dari TCP dan UDP di jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* OSPF, RIPv2 dan BGP.
2. Dapat menjadi referensi bagi *Network Administrator* untuk menentukan teknologi yang akan digunakan sesuai dengan kebutuhannya.
3. Dapat menjadi referensi untuk penelitian yang akan dilakukan selanjutnya.

1.6 Sistematika Penulisan

Untuk mencapai tujuan yang diinginkan, adapun sistematika penulisan yang disusun dalam tugas akhir ini dibagi menjadi lima bab sebagai berikut :

1. Bab I Pendahuluan

Bab ini berisi latar belakang dari penelitian yang dilakukan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

2. Bab II Tinjauan Pustaka dan Dasar Teori

   Pada Bab ini membahas beberapa tinjauan pustaka yang berupa hasil penelitian sebelumnya yang dijadikan acuan dalam penelitian atau penulisan tugas akhir ini. Selain itu dijelaskan juga teori-teori yang mendukung dan berkaitan dengan penelitian tugas akhir ini.

3. Bab III Metodologi Penelitian

   Bab ini berisi langkah-langkah penelitian yang akan dilakukan, rancangan topologi yang akan digunakan, dan skenario pengujian.

4. Bab IV Hasil dan Pembahasan

   Bab ini membahas hasil pengujian berdasarkan skenario pengujian yang telah dilakukan.

5. Bab V Penutup

   Bab ini merupakan bagian terakhir yang berisi kesimpulan dan saran yang dapat dijadikan acuan untuk penelitian selanjutnya.

BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Penelitian [1] melakukan analisis dan perbandingan dari protokol *routing* OSPF dan RIPv2 pada jaringan MPLS dan Non-MPLS berdasarkan variasi jumlah *router* yang digunakan. Pada penelitian ini pengujian dilakukan dengan membebani paket menggunakan UDP. Berdasarkan hasil pengujian yang telah dilakukan pada jaringan Non-MPLS, protokol *routing* OSPF dan RIPv2 menghasilkan nilai QoS yang buruk dengan bertambahnya jumlah *router*. Dilihat berdasarkan parameter ITU-T nilai parameter QoS *packet loss* dari hasil pengukuran didapatkan nilai sebesar 90 % termasuk kategori buruk pada protokol OSPF dan 83% pada protokol RIPv2. Sedangkan pada jaringan MPLS nilai QoS pada protokol RIPv2 menghasilkan nilai *bitrate* 36.40%, *jitter* 15.14% dan *packet loss* 12%. Pada protokol OSPF nilai *bitrate* sebesar 36.86%, *jitter* 20.65% dan *packet loss* sebesar 8%.

Penelitian [2] melakukan implementasi dan analisis sistem keamanan dengan menggunakan IP *Security* (IPSec) di dalam MPLS-VPN pada jaringan IP *Multimedia System* (IMS). Berdasarkan pengujian yang telah dilakukan terhadap keamanan dengan melakukan serangan DoS, didapatkan hasil QoS bahwa nilai *jitter* dan *delay* tidak terpengaruh serangan. Namun nilai *packet loss* sebesar 30 % dimana hal tersebut berarti melewati batas toleransi dari standar ITU-T G.104 bahwa maksimal *packet loss* adalah sebesar 20%.

Penelitian [3] melakukan analisis dan perbandingan antara protokol TCP, UDP dan SCTP pada lalu lintas multimedia. Berdasarkan penelitian yang dilakukan didapatkan beberapa hasil yaitu nilai *Maximum Flow*, nilai *Total Frames Transfer* dan nilai *Total Data Transfer*. *Maximum Flow* merupakan kemampuan protokol untuk melakukan komunikasi multimedia yang mana semakin besar menandakan semakin baik, dimana nilai dari *Maximum Flow* yaitu TCP 106 *Frame*/s, UDP 103 *Frame*/s dan SCTP 159 *Frame*/s. Total *Frames Transfer* adalah total *frame* yang berhasil ditransfer selama 120 detik (waktu yang digunakan dalam penelitian), dimana semakin besar *frame* yang diterima berarti akan menghasilkan video yang bagus. Hasil dari Total *Frame*s *Transfer* yaitu TCP

6487, UDP 6574 dan SCTP 7049. Total Data Transfer adala data yang berhasil ditransfer atau diterima oleh protokol, dimana hasilnya yaitu TCP 4.54 MB, UDP 4.48 MB dan SCTP 4.59 MB. Berdasarkan hasil yang didapatkan dari penelitian tersebut, maka dapat disimpulkan bahwa protokol SCTP lebih bagus untuk lalu lintas multimedia dari pada TCP dan UDP. Tetapi SCTP tidak baik digunakan untuk aktivitas sehari-hari karena akan menggunakan *Throughput* yang besar. Protokol TCP merupakan protokol yang paling stabil dan bisa digunakan untuk aktivitas secara bersamaan seperti memutar *video streaminng* dengan *browsing* dan lain-lain.

Penelitian [4] berkaitan dengan analisis kerja audio dan *video streaming* pada jaringan MLS-VPN berbasis IPSec. Berdasarkan hasil penelitian tersebut diperoleh hasil bahwa secara keseluruhan performa dari jaringan yang menerapkan MPLS lebih unggul dari pada jaringan tanpa MPLS dan MPLS-VPN. Dalam pengiriman sebuah *file*, jaringan MPLS memerlukan waktu 23 s. Waktu yang diperlukan paling sedikit dari pada jaringan tanpa MPLS yang memerlukan 24 s dan MPLS VPN yang memerlukan 40 s.

Penelitian [5] berkaitan dengan analisis pengaruh IPSec pada keamanan jaringan. Penelitian ini fokus dalam menganalisis fitur keamanan jaringan dalam Microsoft Windows dengan mengimplementasikan IPSec. Hasil dari penelitian tersebut yaitu dengan menggunakan IPSec keamanan pada jaringan komputer akan meningkat karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Jika terjadi penyadapan, maka data asli tidak dapat dilihat dengan mudah tanpa mengetahui kunci enkripsi dari data yang dikirim tersebut. Penelitian ini dapat menjadi referensi bahwa IPSec dapat meningkatkan keamanan jaringan yang nantinya akan dikombinasikan dengan jaringan MPLS yang akan digunakan.

Penelitian [6] melakukan analisis perbandingan waktu dan kecepatan transfer pada *Multiprotocol Label Switching* (MPLS) dengan *Virtual Private Network* (VPN) untuk perpindahan dokumen pada jaringan komputer. Pengujian dilakukan dengan menggunakan tiga *routing protocol* yaitu LDP, BGP dan OSPF. Dari pengujian yang telah dilakukan, perbandingan waktu yang dibutuhkan yaitu jaringan MPLS membutuhkan waktu 4,81 detik, dimana lebih cepat 105,70 detik

daripada jaringan VPN yang membutuhkan waktu 110,51 detik. Sedangkan hasil perbandingan kecepatan transfer didapatkan bahwa jaringan MPLS lebih cepat dari pada jaringan VPN. Nilai rata-rata kecepatan transfer jaringan MPLS sebesar 36,12 Mbps sedangkan pada jaringan VPN sebesar 0,10 Mbps.

Berdasarkan pemaparan tinjauan pustaka di atas, maka dalam tugas akhir ini akan dilakukan penelitian terhadap perbandingan *Quality of Service* (QoS) TCP dan UDP pada jaringan MPLS dengan Non-MPLS menggunakan *tunneling* L2TP/IPSec berdasarkan tiga protokol *routing* yaitu OSPF, RIPv2 dan BGP. Penelitian ini dilakukan dikarenakan masih kurangnya referensi penelitian dalam membandingkan kinerja TCP dan UDP pada jaringan MPLS. Dengan adanya penelitian ini diharapkan dapat memberikan referensi tambahan bagi para administrator jaringan dalam menentukan teknologi yang akan digunakan sesuai dengan kebutuhannya.

2.2 Dasar Teori

2.2.1 OSI *Layer Model*

OSI *Reference Model for open networking* atau model referensi jaringan terbuka OSI adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan *International Organization for Standardization* (ISO) di Eropa pada tahun 1977. OSI sendiri merupakan singkatan dari *Open System Interconnection*.

Model ini disebut juga dengan "Model tujuh lapis OSI" (OSI *seven layer model*). Model OSI dibuat untuk mengatasi berbagai kendala *internetworking* akibat perbedaan arsitektur dan protokol jaringan. Dahulu, komunikasi antar komputer dari vendor yang berbeda sangat sulit dilakukan. Masing-masing vendor menggunakan protokol dan format data yang berbeda-beda. Sehingga *International Organization for Standardization* komunikasi (ISO) yang membuat dikenal sebagai suatu *Open Architecture System Interconnection* (OSI) model yang mendefinisikan standar untuk menghubungkan komputer-komputer dari vendor yang berbeda [3]. *Layer* pada model OSI ditunjukkan pada Tabel 2.1.

Tabel 2.1 OSI Layer

Layer	**Fungsi**	**Contoh Protokol**

Aplication	Menyediakan servis bagi berbagai aplikasi *network*	NNTP, H7, Modbus, SIP, SSI, DHCP, FTP, Gopher, HTTP, NFS, NTP. RTP, SMPP, SMTP, Telnet
Presentation	Mengatur konversi dan translasi berbagai format data, seperti kompresi data dan enkripsi data	TDI, ASCII, EBCDIC, MIDI, MPEG, ASCII7
Session	Mengatur sesi (*session*) yang meliputi *estabilishing* (memulai sesi), *maintaining* (mempertahankan sesi) dan *terminating* (mengakhiri sesi) antar entitas yang dimiliki oleh *presentation layer*	SQL, X Windows, DNS, NetBIOS, ASP, SCP, OS Scheduling, RPC, NFS, ZIP
Transport	Menyediakan *end to end communication protocol*. *Layer* ini bertanggung jawab terhadap "keselamatan data" seperti mengatur *flow control* (kendali aliran data), *error detection* (deteksi error) dan *correction* (koreksi), *data secuencing* (urutan data) dan *size of the packet* (ukuran data)	TCP, SPX, UDP, SCTP, IPX
Network	Menentukan rute yang dilalui oleh data. *Layer* ini menyediakan *logical addressing* (pengalamatan logika) dan *path determination* (penentuan rute tujuan)	IP, ICMP, IPSec, ARP. RIP, IGRP, BGP, QSPF, NBF, Q.931

Data Link	Menentukan pengalamatan fisik (*hardware address*), *error* notifikasi (pendeteksi *error*), *frame flow control* (kendali aliran *frame*) dan topologi aliran *network* Ada dua *sub layer* pada data *link*, yaitu *Logical Link Control* (LLC) dan Media *Access Control* (MAC) LLC mengatur komunikasi, seperti *error notification* dan *flow control*. Sedangkan MAC mengatur pengalamatan fisik yang digunakan dalam proses komunikasi antar adapter	802.3 (*Ethernet*) 802.11 a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, CDP, HDP, FDDI, Fibre *Channel Frame* Relay, SDLC, HDLC, ISL, PPP Q.921, *Token Ring*
Physical	Layer ini menentukan masalah kelistrikan / gelombang / medan dan berbagai prosedur / fungsi yang berkaitan dengan link fisik, seperti besar tegangan / arus listrik, panjang maksimal media transmisi, pergantian fasa, jenis kabel dan konektor	RS.232, V.35, V.34, L430, L.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, DSL, 802.11a/b/g/n PHY, Hub, Repeater, Fibre, Optics

2.2.2 *Layer Transport*

Layer transport ini terdapat 2 protokol utama yaitu protokol UDP (*User Datagram Protocol*) dan protokol TCP (*Transmission Control Protokol*). Protokol ini untuk mendukung konsep jaringan berbasis IP. Telah diketahui bahwa IP (*internet protocol*) sebagai protokol 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 [2].

2.2.3 *Transmission Control Protocol* (TCP)

TCP adalah protokol yang dapat dipercaya dan dirancang untuk menyediakan alur data pada jaringan internet yang secara umum diketahui dengan kondisi tidak dapat dipercaya serta dirancang untuk beradaptasi dengan peralatan jaringan terhadap berbagai macam permasalahannya. Dirancangnya protokol ini untuk dapat dipercaya maka TCP bersifat *connection oriented* dalam mengirimkan data. TCP menjamin data yang terpercaya dengan menggunakan ARQ (*Automatic Repeat Request*). ARQ akan mentransmisikan secara otomatis berdasarkan informasi gagal diterimanya data ACK (*Acknoledgement*) dari penerima data. Untuk menjamin kontrol efektif terhadap hambatan maka dilakukan dengan cara mengestimasi *delay* dari transmisi *round trip time* secara akurat, sehingga dengan mempergunakan informasi balasan dari jaringan tersebut maka dapat mendeteksi sebuah kemacetan jaringan dan menyelesaikannya. Penjelasan TCP dapat ditemui pada RFC 793, 1122 dan 1323.

TCP memiliki tujuh fitur utama yaitu sebagai berikut:

1. *Connection oriented*, aplikasi meminta koneksi dan menggunakannya dalam transfer data.
2. *Point-to-point communication*, setiap koneksi TCP memiliki pasti dua titik.
3. *Reliability*, TCP menjamin bagi data yang dikirimkan dalam koneksi dapat terkirim dengan pasti tanpa ada yang hilang atau dobel.
4. *Full-duplex connection*, koneksi TCP memperbolehkan data untuk berkoneksi dari salah satu titik koneksi setiap saat.
5. *Stream interface*, TCP memperbolehkan aplikasi untuk mengirimkan koneksi yang berkesinambungan.
6. *Reliable startup*, membutuhkan persetujuan dari kedua aplikasi untuk melakukan koneksi baru.
7. *Graceful shutdown*, aplikasi dapat membuka aplikasi, mengirim data dan menutup koneksi serta menjamin bahwa data sampai sebelum koneksi terputus [3].

2.2.4 *User Datagram Protocol* (UDP)

Protokol ini untuk mendukung konsep jaringan berbasis IP. Telah diketahui bahwa IP (*internet protocol*) sebagai protokol 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.

Berbeda dengan TCP, protokol UDP adalah protokol yang bersifat *connectionless* dalam mentransmisi data dan tidak mengenal dalam pengecekan terhadap *error* pengiriman data. Protokol UDP pada dasarnya hanya mengandung IP dengan tambahan *header* singkat. Protokol UDP tidak melakukan sebuah proses kontrol alur data, kontrol kesalahan ataupun pengiriman ulang terhadap kesalahan sehingga hanya menyediakan interface ke protokol IP. UDP sangat berguna sekali pada situasi *client-server* dan penjelasan UDP lebih detil dapat ditemui pada RFC 768.

UDP memiliki karaketeristik yaitu sebagai berikut:

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* [3].

2.2.5 Jaringan *Multiprotocol Label Switching* (MPLS)

Multiprotocol Label Switching (MPLS) merupakan sebuah teknik yang menggabungkan kemampuan manajemen *switching* yang ada dalam teknologi ATM dengan fleksibilitas *network layer* yang dimiliki teknologi IP. Fungsi *label* pada MPLS adalah sebagai proses penyambungan dan pencarian jalur dalam jaringan komputer. MPLS menggabungkan teknologi *switching* di *layer 2* dan teknologi *routing* di *layer 3* sehingga menjadi solusi jaringan terbaik dalam menyelesaikan masalah kecepatan, *scalability,* QOS *(Quality of Service)*, dan rekayasa trafik. Dengan informasi *label switching* yang didapat dari *routing*

network layer, setiap paket hanya dianalisa sekali di dalam *router* dimana paket tersebut masuk ke dalam jaringan untuk pertama kali. *Router* tersebut berada di tepi dan dalam jaringan MPLS yang biasa disebut dengan *Label Switching Router* (LSR).

Ide dasar teknik MPLS ini ialah mengurangi teknik pencarian rute dalam setiap *router* yang dilewati setiap paket, sehingga sebuah jaringan dapat dioperasikan dengan efisien dan jalannya pengiriman paket menjadi lebih cepat. Jadi MPLS akan menghasilkan *high-speed routing* dari data yang melewati suatu jaringan yang berbasis parameter *Quality of Service* (QoS) [4].

Keuntungan MPLS

a. Mengurangi banyaknya proses pengolahan di IP *Router*s, serta memperbaiki proses pengiriman suatu paket data.
b. Menyediakan QoS dalam jaringan *backbone*, sehingga setiap layanan paket yang dikirimkan akan mendapat perlakuan sesuai skala prioritas.

2.2.6 *Tunneling* L2TP/IPSec

L2TP merupakan *tunneling protocol* yang memadukan dua buah *tunneling* protokol yaitu *Layer* 2 *Forwarding* milik Cisco dan PPTP yang dimiliki Microsoft. L2TP umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang dapat membawa semua jenis protokol komunikasi di dalamnya dan biasanya menggunakan *port* 1702 dengan protokol UDP.

IPSec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec bekerja dengan tiga cara yaitu: *Network-to-network, Host-to-network dan Host-to-host.*

IPSec adalah pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya. Pada dasarnya paket IP tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditransmisikan oleh si pengirim paket. Paket IP yang tidak memiliki keamanan atau *security*, sangat mudah untuk diketahui isinya dan alamat IP itu sendiri. IPsec adalah metode yang bertujuan

untuk menjaga keamanan IP datagram ketika paket diransmisikan pada *traffic*. Sehingga Ipsec menjadi suatu mekanisme yang diimplementasikan pada VPN. IPSec berada pada *layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada di atasnya [7]. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec.

2.2.7 *Routing Protocol*

Routing protocol adalah suatu aturan yang mempertukarkan informasi *routing* yang akan membentuk sebuah tabel *routing* sehingga pengalamatan pada paket data yang akan dikirim menjadi lebih jelas dan *routing protocol* mencari rute tersingkat untuk mengirimkan paket data menuju alamat yang dituju.

Fungsi utama dari *layer network* adalah pengalamatan dan routing, routing merupakan fungsi yang bertanggung jawab membawa data melewati sekumpulan jaringan dengan cara memilih jalur terbaik untuk dilewati data. Algoritma routing yang menentukan pilihanmelalui jaringan itu, tergantung metode yang digunakan untuk membagi informasi *external*, dimana algoritma sebagai metode yang digunakan untuk memproses informasi *internal* [8].

1. *Distance vector*

Sebuah distance *vector protocol* menginformasikan banyaknya hop ke jaringan tujuan (*the distance*) dan arahnya dimana sebuah paket dapat mencapai jaringan tujuan (*the vector*). Algoritma *distance vector*, juga dikenal sebagai algoritma Bellman-Ford, router mampu untuk melewatkan *updates routeke* tetanggganya pada interval rutin terjadwal. Setiap tetangga kemudian menerima nilai tujuannya sendiri dan menyalurkan informasi routing ke tetangga terdekat. Hasil dari proses ini sebuah tabel yang berisi kumpulan semua *distance*/tujuan ke semua jaringan tujuan. Beberapa protokol yang termasuk Distance Vector yaitu RIP dan BGP [8].

2. *Link state*

Routing ini menggunakan teknik *link state*, dimana artinya tiap *router* akan mengumpulkan informasi tentang *interface*, *bandwidth*, *roundtrip* dan sebagainya. Kemudian antar *router* akan saling menukar informasi, nilai yang paling efisien yang akan diambil sebagai jalur dan di masukkan ke dalam *table routing*. Dengan

menggunakan algoritma pengambilan keputusan *Shortest Path First* (SPF), informasi LSA tersebut akan diatur sedemikian rupa hingga membentu suatu jalur routing. Protokol yang menggunakan algoritma ini yaitu OSPF [8].

3. *Hybrid*

Protokol *hybrid* menggunakan aspek-aspek dari *routing* protokol jenis *distance-vector* dan *routing* protocol jenis *link-state* sebagai contoh adalah EIGRP.

2.2.8 *Open Shortest Path First* (OSPF)

Open Shortest Path First (*OSPF*) merupakan *protocol routing link state* dan digunakan untuk menghubungkan *router-router* yang yang berada dalam satu *Autonomus System* (*AS*), sehingga *protocol routing* ini termasuk juga dalam kategori *Interior Gateway Protocol* (*IGP*). *OSP*F dikembangkan untuk menutupi kekurangan-kekurangan yang dimiliki oleh RIP, terutama pengimplementasian di jaringan berskala besar, *RIP* mempunyai kekurangan dalam kecepatan mencapai kondisi konvergensi untuk jaringan berskala besar. Untuk dapat menangani jaringan yang berskala besar, maka *OSP*F menerapkan konsep area dalam implementasinya, yaitu *Single Area* untuk jaringan berskala kecil dan *Multi Area* untuk jaringan berskala besar. *Router* yang menjalankan *OSPF* hanya akan bertukar informasi *route* (*routing update*) dengan *router OSPF* lainnya yang berada dalam satu *Autonomus System* (*AS*). *Router* OSPF akan mengirimkan beberapa paket *OSPF* lainnya yang ke semuanya digunakan membentuk table *routing*. Pada *OSPF* dikenal kondisi adjency antar *router*. Sebelum *router-router* tersebut bertukar informasi *routing*, maka sebuah *router* harus terlebih dahulu mencapai kondisi *adjency* (bertetangga dan bersepakat) dengan *router* tetangganya. *Router-router* tidak akan bertukar *routing update* jika kondisi *adjency* belum tercapai [9].

2.2.9 *Routing Information Protoco*l version 2 (RIPv2)

*Routing Information Protoco*l (RIP) mengirim *routing table* yang lengkap ke semua *interface* yang aktif setiap 30 detik. RIP hanya menggunakan jumlah *hop* untuk menentukan cara terbaik ke sebuah *network remote*, tetapi RIP secara *default* memiliki sebuah nilai jumlah *hop* maksimum yg diizinkan, yaitu 15, berarti nilai 16 tidak terjangkau (*unreachable*). RIP bekerja baik pada jaringan

kecil, tetapi RIP tidak efisien pada jaringan besar dengan link WAN atau jaringan yang menggunakan banyak *router*.

2.2.10 *Border Gateway Protocol* (BGP)

Border Gateway Protocol (BGP) Merupakan *distance vector exterior gateway protocol* yang bekerja secara cerdas untuk merawat *path-path* ke jaringan lainnya. *Update-update* dikirim melalui koneksi TCP.

2.2.11 *Quality of Services* (QoS)

Quality of Service (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan *bandwidth*, mengatasi *jitter* dan *delay* di berbagai macam teknologi meliputi jaringan IP dan lainnya. *QoS* didesain untuk membantu *end user* (*client*) menjadi lebih *produktif* dengan memastikan bahwa *user* mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. Tujuan dari QoS adalah untuk memenuhi kebutuhan – kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama [10].

Ada beberapa parameter QoS yang akan digunakan dalam penelitian ini, yaitu :

1. Throughput

Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. *Throughput* merupakan kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* selalu dikaitkan dengan *bandwidth* karena *throughput* memang bisa disebut juga dengan *bandwidth* dalam kondisi yang sebenarnya. *Bandwidth* lebih bersifat *fix* sementara *throughput* sifatnya adalah dinamis tergantung trafik yang sedang terjadi [11]. Berikut ini merupakan kategori *throughput* sesuai dengan standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) yang dapat dilihat pada Tabel 2.2.

Tabel 2.2 Kategori *Throughput*

Kategori *Throughput*	*Throughput* (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3

Sedang	50	2
Jelek	<25	1

Persamaan perhitungan *Throughput* :

$$Throughput = \frac{\text{Paket data diterima}}{\text{Lama Pengamatan}}$$

2. Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Untuk mengetahui nilai *delay* rata – rata adalah dengan melihat lama waktu yang digunakan dan total paket yang diterima [11]. Berikut ini merupakan kategori *delay* sesuai dengan standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) yang dapat dilihat pada Tabel 2.3.

Tabel 2.3 Kategori *Delay*

Kategori *Delay*	*Delay* (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 s/d 300	3
Sedang	300 s/d 450	2
Jelek	<450	1

Persamaan perhitungan *Delay* :

$$Delay = \frac{Packet\ Length}{Link\ Bandwidth}$$

3. Jitter

Jitter atau variasi kedatangan paket, merupakan masalah khas dari *connectionless network* atau *packet switched network*. *Jitter* didefinisikan sebagai variasi *delay* antar paket yang diakibatkan oleh panjang *queue* dalam suatu pengolahan data dan *reassemble* paket – paket data di akhir pengiriman akibat kegagalan sebelumnya. *Delay* antrian pada *router* dan *switch* dapat menyebabkan *jitter*. Semakin besar beban trafik atau nilai variasi *delay* di dalam jaringan akan menyebabkan semakin besar pula peluang terjadinya tumbukan antar paket, sehingga nilai *jitter* akan semakin besar dan menyebabkan nilai QoS semakin

turun. Berikut ini merupakan kategori *jitter* sesuai dengan standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) yang dapat dilihat pada Tabel 2.4.

Tabel 2.4 Kategori *Jitter*

Kategori *Jitter*	*Jitter* (ms)	Indeks
Sangat Bagus	0	4
Bagus	0 s/d 75	3
Sedang	75 s/d 125	2
Jelek	125 s/d 225	1

Persamaan perhitungan *Jitter* :

$$Jitter = \frac{\text{Total variasi } delay}{\text{Total paket yang diterima}}$$

Total Variasi *Delay* = *Delay* – (rata-rata *delay*)

2.2.12 *Graphic Network Simulator version 3* (GNS3)

Graphic Network Simulator version 3 (GNS3) adalah *open source* (GNU GPL) perangkat lunak yang dapat mensimulasikan jaringan dengan masalah yang kompleks dan mendekati dari cara jaringan nyata, semua ini tanpa didedikasikan perangkat keras jaringan seperti *router* dan switch (Joko Saputro, 2010:4). GNS3 itu sendiri adalah sebuah program *graphical network simulator* yang dapat mensimulasikan topologi jaringan yang lebih kompleks dan sangat mudah diakses hanya "*plug and play*" dibandingkan dengan simulator lainnya. GNS3 menyediakan antar muka penggunaaan grafis untuk merancang dan mengkonfigurasi di jaringan virtual, itu berjalan pada *hardware* PC dan dapat digunakan pada beberapa sistem platform operasi termasuk Windows, Linux, dan Mac OS X. Dalam memberikan simulasi yang lengkap dan akurat , GNS3 adalah emulator untuk menjalankan sistem operasi yang sama seperti pada jaringan nyata [9].

2.2.13 Virtual Box

Oracle VM VirtualBox (*Virtual Machine*) atau yang biasa sering disebut dengan vbox atau virtualbox. Aplikasi virtualbox dikembangkan oleh Oracle. Awal mula aplikasi ini pertama kali dikembangkan oleh perusahaan Jerman,

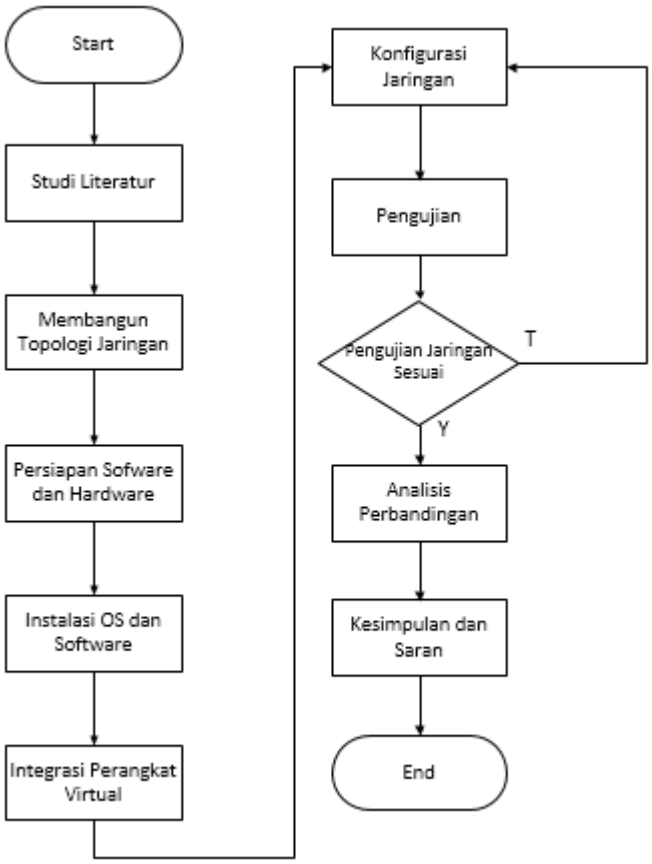
Innotek GmbH. Februari 2008, Innotek GmbH kemudian diakusisi oleh Sun Microsystems. Dan pada akhirnya Sun Microsystems juga diakuisisi oleh Oracle.

Virtualbox merupakan suatu alat perangkat lunak secara virtualisasi, yang dapat digunakan untuk mengeksekusi suatu sistem operasi tambahan di dalam sistem operasi utama. Fungsi ini penting jika seseorang ingin melakukan uji coba dan melakukan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada. Aplikasi dengan fungsi sejenis VirtualBox lainnya adalah Vmware dan Microsoft Virtual PC [9].

BAB III
METODOLOGI PENELITIAN

3.1 Diagram Alir

Dari penelitian yang akan dilakukan terdapat beberapa langkah-langkah atau proses yang akan dilakukan. Langkah-langkah tersebut dapat dilihat pada **Gambar 3.1**.



Gambar 3.1 Diagram Alir Penelitian

Pada **Gambar 3.1** merupakan diagram alir yang menggambarkan langkah-langkah dari penelitian yang dilakukan. Terdapat sembilan langkah penelitian yang akan dilakukan, yaitu studi literatur, membangun topologi jaringan, persiapan *hardware* dan *software*, instalasi OS dan *software*, intergrasi perangkat virtual, konfigurasi jaringan, pengujian, analisis perbandingan, serta kesimpulan dan saran. Pada tahap pengujian, jika pengujian yang dilakukan sudah sesuai dan tidak ada error atau kesalahan, maka dapat dilanjutkan ke tahap aanalisis perbandingan. Tetapi jika pada pengujian terdapat kesalahan, maka kembali lagi

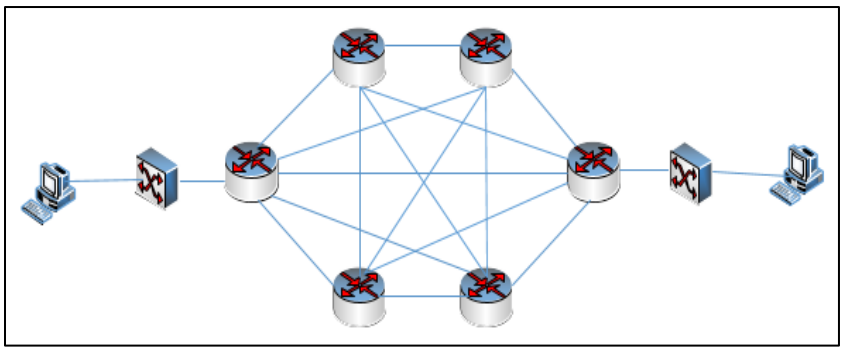
ke tahap konfigurasi jaringan untuk melakukan konfigurasu ulang terhadap jaringan yang akan diuji.

3.2 Studi Literatur

Mempelajari literatur yang berkaitan dengan penelitian ini, yaitu seperti literatur tentang TCP dan UDP, jaringan MPLS, *tunneling* L2TP/IPSec, protokol *routing* OSPF, RIPv2 dan BGP. Berdasarkan hasil dari studi literatur yang telah dilakukan, diharapkan dapat membantu dalam pengerjaan penelitian ini.

3.3 Membangun Topologi Jaringan

Pada tahapan ini dilakukan pembuatan desain topologi jaringan yang akan digunakan dalam penelitian ini. Topologi jaringan yang digunakan pada penelitian ini dapat dilihat pada **Gambar 3.2**.



Gambar 3.2 Topologi jaringan

Pada **Gambar 3.2** merupakan topologi jaringan yang digunakan pada penelitian ini. Topologi yang digunakan yaitu topologi *mesh* dengan enam buah *router*, dua buah *switch* dan dua buah komputer yang masing-masing sebagai *client* dan *server*. Topologi *mesh* digunakan karena memiliki keamanan yang tergolong baik, tidak ada tabrakan data, pengiriman dan pemrosesan data juga tergolong cepat [12]. Sehingga akan mendukung kinerja dari jaringan MPLS saat dilakukan perbandingan terhadap TCP dan UDP.

3.4 Persiapan *Hardware* dan *Software*

Untuk melakukan penelitian ini memerlukan beberapa *hardware* dan *software* yang dapat mendukung penelitian ini. *Hardware* dan *software* yang dibutuhkan adalah sebagai berikut :

1. *Hardware*

   Hardware yang digunakan dalam penelitian ini yaitu sebuah laptop dengan *processor* intel(R) celeron(R) CPU N3060 @1.60Hz 1.60 GHz RAM 4 GB.

2. *Software*

Software yang digunakan pada penelitian ini yaitu :

a. Simulator GNS3 sebagai *Network Simulator*.
b. Linux Ubuntu LTS 14.0 sebagai sistem operasi yang digunakan pada penelitian ini.
c. Virtual Box sebagai *tools* untuk melakukan instalasi perangkat virtual.
d. Wireshark sebagai *Network Analyzer* untuk memonitoring *traffic* paket data yang melewati jaringan.
e. Iperf sebagai alat untuk mengukur QoS dengan parameter *Throughput*, *Delay* dan *Jitter*.

3.5 Instalasi OS, *Software* dan Qemu *Router*

Pada tahapan ini dilakukan instalasi semua *software* yang akan digunakan untuk melakukan penelitian ini. Instalasi *software* dimulai dengan menginstal simulator GNS3, kemudian VirtualBox untuk membuat OS virtual. OS yang akan digunakan yaitu Linux Ubuntu LTS 14.0. Kemudian melakukan instalasi Wireshark sebagai *network analyzer* dan Iperf sebagai *tool* untuk mengukur nilai QoS. Selanjutnya akan dilakukan instalasi *router* Mikrotik *Cloud Hosted Router* (CHR) sebagai virtual *router* pada GNS3. *Router* OS yang digunakan yaitu versi 6.45.7.

3.6 Integrasi Perangkat Virtual

Pada Tahapan ini perangkat virtual yang telah diinstal akan diintegrasikan dengan simulator GNS3 agar dapat digunakan pada simulator seperti Mikrotik CHR dan VirtualBox. Mikrotik CHR diintegrasikan dengan GNS3 agar virtual *router* dapat digunakan pada simulator. Sedangkan VirtualBox diintegrasikan dengan GNS3 agar OS yang digunakan dapat terhubung dengan simulator GNS3.

3.7 Konfigurasi Jaringan

Pada tahapan ini dilakukan konfigurasi jaringan OSPF, RIPv2 dan BGP pada jaringan Non-MPLS, MPLS dan MPLS dengan *tunneling* L2TP/IPSec. Konfigurasi jaringan dilakukan di masing-masing *router* pada topologi jaringan yang digunakan.

3.8 Pengujian

Setelah dilakukan konfugurasi jaringan, selanjutnya akan dilakukan pengujian terhadap QoS TCP dan UDP pada jaringan. Parameter QoS yang akan diukur yaitu *throughput*, *delay* dan *jitter*. Pengujian ini terdiri dari beberapa skenario, yaitu :

1. Pengujian QoS TCP
   a. Pengujian TCP pada jaringan Non-MPLS dengan protokol *routing* OSPF.
   b. Pengujian TCP pada jaringan Non-MPLS dengan protokol *routing* RIPv2.
   c. Pengujian TCP pada jaringan Non-MPLS dengan protokol *routing* BGP.
   d. Pengujian TCP pada jaringan MPLS dengan protokol *routing* OSPF.
   e. Pengujian TCP pada jaringan MPLS dengan protokol *routing* RIPv2.
   f. Pengujian TCP pada jaringan MPLS dengan protokol *routing* BGP.
   g. Pengujian TCP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* OSPF.
   h. Pengujian TCP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* RIPv2.
   i. Pengujian TCP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* BGP.
2. Pengujian QoS UDP
   a. Pengujian UDP pada jaringan Non-MPLS dengan protokol *routing* OSPF.
   b. Pengujian UDP pada jaringan Non-MPLS dengan protokol *routing* RIPv2.
   c. Pengujian UDP pada jaringan Non-MPLS dengan protokol *routing* BGP.
   d. Pengujian UDP pada jaringan MPLS dengan protokol *routing* OSPF.
   e. Pengujian UDP pada jaringan MPLS dengan protokol *routing* RIPv2.
   f. Pengujian UDP pada jaringan MPLS dengan protokol *routing* BGP.
   g. Pengujian UDP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* OSPF.
   h. Pengujian UDP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* RIPv2.
   i. Pengujian UDP pada jaringan MPLS dengan *tunneling* L2TP/IPSec berdasarkan protokol *routing* BGP.

Pengujian dengan beban paket TCP dilakukan dengan membebani jaringan yang telah dikonfigurasi dengan paket TCP begitu juga dengan UDP. Terdapat perbedaan cara kerja antara TCP dan UDP dalam melakukan transmisi paket data. TCP memiliki karakter yaitu *reliable* dan *connection-oriented*. Dimana *reliable* berarti data yang dikirim menggunakan TCP terdapat jaminan bahwa data tersebut akan sampai ke tujuan dengan utuh atau tidak hilang. Sedangkan *connnection-oriented* berarti pada saat pengiriman data ke penerima akan terjadi proses *handshaking* terlebih dahulu antara pengirim dan penerima agar dapat melakukan sikronisasi terhadap proses *acknowledgement*. Jika pada saat proses transmisi data terjadi kegagalan pengiriman, maka TCP akan otomatis melakukan transmisi ulang.

UDP merupakan protokol yang mengutamakan kecepatan. UDP memiliki karakter yaitu *unreliable* dan *connectionless*. *Unreliable* berarti paket data yang dikirim akan dikirim tanpa adanya nomor urut atau pesan *acknowledgement*, sehingga dapat menyebabkan paket yang diterima bisa saja dalam keadaan tidak lengkap atau tidak urut. *Connectionless* berarti tidak ada aktivitas *handshaking* antara pengirim dan penerima saat akan melakukan pengiriman paket data. Hal ini dapat menyebabkan kemungkinan hilangnya paket data yang akan dikirimkan.

Pengujian pada masing-masing skenario akan dilakukan sebanyak sepuluh kali pengujian. Pada pengujian di masing-masing skenario akan digunakan variasi *bandwidth* sebesar 750 kbps dan 1 Mbps. Mikrotik CHR hanya dapat menampung beban maksimum *bandwidth* sebesar 1 Mbps, oleh karena itu pada pengujian akan digunakan variasi *bandwidth* sebesar 750 kbps dan 1 Mbps.

Setelah masing-masing skenario dilakukan pengujian, maka akan dilakukan pengambilan data hasil pengujian berupa parameter QoS yang digunakan yaitu *throughput*, *delay* dan *jitter* menggunakan *tools* Iperf. Analisis dilakukan dengan memonitoring setiap paket yang melewati jaringan menggunakan Wireshark. Setelah itu akan didapatkan nilai rata-rata parameter QoS yang telah diukur. Nilai rata-rata parameter QoS tersebut kemudian akan disajikan dalam bentuk grafik dan akan dilakukan perbandingan hasil QoS berupa *throughput, delay,* dan *jitter* dari TCP dan UDP pada masing-masing skenario.

3.9 Rencana Pelaksanaan Penelitian

Berikut ini merupakan rencana pelaksanaan penelitian yang dapat dilihat pada Tabel 3.1.

Tabel 3.1 Rencana Pelaksanaan Penelitian11

No.	Kegiatan	Bulan I				Bulan II				Bulan III				Bulan IV				Bulan V				Bulan VI			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Studi Literartur																								
2.	Membangun Topologi Jaringan																								
3.	Persiapan *Software* dan *Hardware*																								
4.	Instalasi OS dan *Software*																								
5.	Integrasi Perangkat Virtual																								
6.	Konfigurasi Jaringan																								

7.	Pengujian																							
8.	Analisis Perbandingan																							
9.	Dokumentasi																							

DAFTAR PUSTAKA

[1] D. Supriadi, “Analisis Perbandingan Protokol *Routing* OSPF DAN RIPv2 Berdasarkan Variasi Jumlah Router Pada Jaringan MPLS Dan Tanpa MPLS Menggunakan Simulator GNS3,” J-COSINE, Vol. 3, No. 1, Pp. 10–18, 2019.

[2] R. Arlan, “Implementasi Dan Analisis Sistem Keamanan *IP Security* (IPSec) Di Dalam M*ulti Protocol Label Switching-Virtual Private Network* (MPLS-VPN) Pada Layanan Berbasis *IP Multimedia Subsystem* (IMS),” Open Library Telkom University, Vol. 3, No. 3, Pp. 4630–4640, 2016.

[3] Y. Mardiana, “Analisa Performansi Protokol TCP, UDP dan SCTP Pada Lalu Lintas Multimedia,” Jurnal Media Infotama, Vol. 13, No. 2, Pp. 73–84, 2017.

[4] M. Z. S. Hadi, “Analisa Unjuk Kerja *Audio* dan *Video Streaming* Pada Jaringan MPLS VPN Berbasis IPSec.” Industrial Electronic Seminar, 2010.

[5] S. Hidayatulloh, “Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSec,” Jurnal Informatika Fakultas Teknik dan Informatika Universitas Bina Sarana Informatika, Vol. I, No. 2, Pp. 93–104, 2014.

[6] I. Saleh,"Analisa Perbandingan Waktu dan Kecepatan Transfer pada Multi Protocol Label Switching (Mpls) dengan Virtual Private Network (Vpn) untuk Perpindahan Dokumen pada Jaringan Komputer." *Compiler*, vol. 3, no. 1, Pp. 101–112, 2014.

[7] W. O. Zamalia, L. M. F. Aksara, M. Yamin, J. T. Informatika, F. Teknik, And U. H. Oleo, “Analisis Perbandingan Performa QoS, PPTP , L2TP , SSTP Dan IPSec Pada Jaringan VPN Menggunakan Mikrotik,” semanTIK Vol. 4, No. 2, Pp. 29–36, 2018.

[8] M. Fatkhurrokhman, “Analisis Perbandingan Metode *Routing Link State* Vs *Distance Vector*,” Retrieved from www.academia.edu, 2013.

[9] A. Puji Adi, Asmunin, Kusuma, “Implementasi *Simple Port Knocking* Pada *Dynamic Routing* (OSPF) Menggunakan Simulasi GNS3,” Jurnal Mahasiswa UNESA, Pp. 7–17, 2016.

[10] Y. Andri, Pranata, I. Fibriani, And S. B. Utomo, “Analisis Optimasi

Kinerja *Quality of Service* Pada Layanan Komunikasi data Menggunakan Ns - 2 di Pt . PLN (PERSERO) Jember," SINERGI, vol.20, no.2, Pp. 149–156, 2016.

[11] R. Wulandari, "Analisis QoS (*Quality Of Service*) Pada Jaringan Internet (Studi Kasus : Upt Loka Uji Teknik Penambangan Jampang Kulon – Lipi)," JUTISI, vol. 2, no.2, pp. 162–172, 2016.

[12] A.A. Wijaya, "Mengenal Berbagai Macam Topologi Jaringan Serta Kelebihan dan Kekurangannya". Retrieved from www.ilmukomputer.org, 2013.