BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam penelitian ini akan digunakan lima tinjauan pustaka yang nantinya dapat mendukung penelitian, berikut ini merupakan tinjauan pustaka yang diambil, yaitu :

1. Menurut (Mohammad Idhom dkk, 2020), judul penelitian "Analisa *Performansi* Routing Protokol RIPv2 Pada Jaringan VPLS". Pada penelitian ini penulis membahas jaringan multicast VPLS (Virtual Private LAN Service) routing RIPv2. VPLS merupakan teknologi yang bersifat *point to multipoint* sehingga penggunaannya pada *video streaming* merupakan langkah yang tepat karena *video streaming* merupakan layanan *point to multipoint*. VPLS memiliki kelebihan pada kecepatan transfer data yang tinggi karena VPLS menggunakan teknologi MPLS (*multi protocol label switching*) sebagai jaringan backbone-nya. MPLS adalah salah satu metode yang di gunakan untuk *turning* jaringan agar dapat meningkatkan kualitas jaringan yang lebih baik sebagai layanan *streaming*. skalabilitas serta menghasilkan fleksibilitas jaringan yang tinggi. Parameter yang akan diuji yaitu *delay, packet loss, jitter dan throughput*. Hasil rata-rata dari client PC dengan jenis jaringan multicast VPLS RIPv2 mendapatkan hasil *throughput* 1.077 Mbit/sec, *delay* 12.75 msec, *jitter* 0.08125 msec, *packet loss* 0.1. Semakin kecil nilai *Packet Loss, jitter, Delay* dan semakin besar nilai *throughput* maka semakin bagus kinerja routing protokol pada video streaming tersebut.
2. Menurut (Novaldy Refi Nugita dan Wiwin Sulistyo, 2022), judul penelitian "Analisis QoS *Streaming* Video Jaringan MPLS Dan VPLS". *Video streaming* merupakan media yang banyak memiliki banyak sekali manfaatnya, terutama untuk pendidikan, pertemuan online, maupun hanya sekedar untuk menonton movie. Berkembangnya jaringan internet dalam tahun demi tahun dapat mempermudah untuk mengakses *video streaming*. MPLS adalah salah satu jaringan internet yang digunakan dikarenakan cepat dalam melakukan transfer data sehingga untuk mengakses *video streaming* menjadi lebih mudah dan juga MPLS menjadi jaringan dasar terbentuknya jaringan VPLS. MPLS

menerapkan pemberian label pada suatu paket data yang dapat meningkatkan kecepatan dalam proses pengiriman data dalam jaringan. Ada juga yang dinamakan VPLS dalam jaringan internet yang memiliki prinsip hampir sama dengan MPLS. Dari dua jaringan yang disebutkan, akan dilakukan uji coba menggunakan *video streaming* dengan parameter QoS diantaranya yaitu *throughput, delay, dan packet loss*. Hasil akhir penelitiani adalah perbandingan kinerja QoS dari jaringan MPLS dan jaringan VPLS, nilai yang didapat antara MPLS dan VPLS adalah 1% hingga 2% untuk kinerja MPLS yang lebih baik dari VPLS.

3. Menurut (Fathurrahmad dan Salman Yusuf, 2019), judul penelitian "Implementasi Jaringan VPN Dengan *Routing Protocol* Terhadap Jaringan *Multiprotocol Label Switching* (MPLS)". *Video streaming* merupakan suatu layanan yang memungkinkan sebuah server untuk mengirimkan video ke beberapa user yang berada pada suatu jaringan. Sebagai contoh layanan video streaming dapat dimanfaatkan untuk *long distance learning*. Untuk menyediakan layanan *long distance learning* dibutuhkan suatu jaringan yang dapat menjaga *privasi client* dan menyediakan jaminan QoS. Hal ini dapat diatasi dengan teknologi *tunneling* pada jaringan *Virtual Private Network* (VPN). Tetapi *tunneling* ini memiliki kelemahan karena kompleksitas jaringan dan mahalnya perangkat yang digunakan. Sehingga lahirlah teknologi *Virtual Private LAN Service* (VPLS) yang dapat mengatasi masalah tersebut. Dengan penambahan teknologi *multicast* pada VPLS diharapkan dapat meningkatkan QoS layanan yang bersifat *point-to-multipoint* seperti *video streaming*.

   Dari hasil pengujian dan analisis implementasi sistem *Multicast* VPLS didapatkan hasil yaitu jaringan VPLS memiliki QoS yang lebih baik daripada jaringan OSPF karena dapat mengurangi *delay* sampai 20.03%, meningkatkan *throughput* sampai 23.13%, dan mengurangi *packet loss* sampai 79.91%. Penambahan teknologi *multicast* terbukti dapat meningkatkan performansi jaringan VPLS yaitu dapat mengurangi *delay* sampai 25.66%, meningkatkan *throughput* 34.27%, tetapi *packet loss* yang dihasilkan oleh *multicast* lebih besar yaitu memiliki selisih sampai 3.54%

dibandingkan *unicast*. Kemudian *bandwidth*, *bitrate*, dan juga jumlah *client* yang mengkases layanan video streaming terbukti mempengaruhi performansi dari jaringan *multicast* VPLS untuk layanan *video streaming*.

4. Menurut (Yanuar Nurdiansyah dkk, 2020), judul penelitian "Analisis Perbandingan Metode *Interior Gateway Protocol* RIP Dengan OSPF Pada Jaringan MPLS-VPLS". *Konvergensi* internet dan telekomunikasi yang berkembang, dengan aplikasi di dalamnya yang semakin tergantung pada ketersediaan *bandwidth* besar, dengan pengaturan QoS-nya membutuhkan jaringan dan elemen di dalamnya yang memberikan dukungan penuh untuk keamanan data dan peningkatan kinerja jaringan. Kebutuhan teknologi pengiriman data yang tidak hanya memfasilitasi perutean dan penemuan lintasan terbaik tetapi juga dapat memberikan keamanan dalam komunikasi data. Penelitian ini membahas implementasi jaringan VPN dengan protokol routing pada jaringan *Multiprotocol Label Switching* (MPLS). Setelah implementasi, kinerja jaringan MPLS akan diuji dan dibandingkan dengan kinerja tanpa MPLS menggunakan model yang direncanakan peneliti. Tujuan khusus dari penelitian ini adalah untuk menunjukkan bagaimana protokol routing memainkan peran penting dalam memperkuat manajemen lalu lintas komunikasi data yang mendukung kemampuan MPLS dari jaringan VPN dan diterapkan pada arsitektur jaringan AMIK Indonesia. Penelitian ini akan menggunakan metode studi literatur yang dimaksudkan untuk memperoleh dan mempelajari data yang terkandung dalam komputer yang terhubung ke jaringan di laboratorium jaringan komputer AMIK Indonesia. Kesimpulan yang didapat dari penelitian ini adalah bahwa MPLS VPN memberikan efisiensi *bandwidth* pada *backbone*, aplikasi jaringan VPN MPLS telah berfungsi secara fungsional sesuai dengan rencana awal penelitian dan penulis juga berhasil mengkonfigurasi jaringan yang berbeda dan memperoleh *bandwidth* yang stabil.
5. Menurut (Raden Aulia Adam Hudaya dan Wiwin Sulistyo, 2018), judul penelitian "Simulasi Perancangan dan Analisis QoS Pada Jaringan MPLS Menggunakan *Tunneling* VPLS". Di era globalisasi, kebutuhan jaringan pada perusahaan dengan kemampuan komunikasi data dengan cepat dan efisien

merupakan kebutuhan yang mutlak. Untuk memenuhi kebutuhan komunikasi data tersebut, perusahaan ISP berusaha menerapkan teknologi tunneling VPLS pada MPLS sebagai jaringan backbone-nya. Pengiriman paket data otomatis secara maksimal mengirim dari node satu ke node yang lain tanpa dipotong header VPN karena menggunakan L2MTU untuk penempatan label sehingga proses distribusi data dapat lebih optimal. Dari hasil pengujian yang dilakukan mampu mengurangi *delay* 19,53%, memaksimalkan *throughput* 20,91%, dan mengurangi *jitter* 34,09% untuk layanan *video streaming*. Sehingga dapat dikatakan MPLS-VPLS memberikan QoS lebih baik daripada EoIP tunnel untuk diterapkan di PT. Grahamedia Informasi Salatiga.

Berdasarkan penelitian terdahulu seperti yang telah diuraikan di atas, menunjukkan bahwa jaringan MPLS-VPLS dapat menjadi salah satu pilihan ketika memerlukan sebuah *tunnel* yang aman. Dengan teknologi VPLS, penyedia layanan juga dapat menghemat biaya karena tidak perlu membeli *IP Public* dengan jumlah yang banyak namun cukup menggunakan satu *IP Public.*

2.2 MikroTik Router OS

MikroTik sebagai produsen perangkat jaringan komputer menghadirkan MikroTik Router OS, sebuah sistem operasi yang dirancang khusus untuk kebutuhan jaringan komputer (Wicahyanto and Sumirat 2012). Fitur utamanya adalah *control network.* MikroTik banyak digunakan oleh perusahaan *Internet Service Provider* (ISP), Perusahaan RT RW net, *Hotspot Provider*, dan lainnya karena menawarkan kemudahan dan keamanan. Selain itu MikroTik tidak membutuhkan perangkat lunak tambahan sebagai perantara berjalannya *Operating System* (OS). Menurut (Hendriyanto Febrian 2011) *MikroTik Router OS* memiliki kelebihan sebagai berikut :

1. Tangguh dalam masalah jaringan
2. *Tools* lebih banyak
3. Sistem Keamanan tingkat tinggi
4. Tidak terlalu membutuhkan spesifkasi komputer yang besar
5. Kemudahan dalam penggunaan dan harga relatif murah

2.3 Fitur MikroTik

1. *Address List* : Pengelompokan IP Address berdasarkan nama.
2. *Asynchronous* : Mendukung serial PPP *dial-in / dial-out*, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, *Radius, dial on demand, modem pool* hingga 128 ports.
3. *Bonding* : Mendukung dalam pengkombinasian beberapa antarmuka *ethernet* ke dalam 1 pipa pada koneksi cepat.
4. *Bridge* : Mendukung fungsi *bridge spinning tree*, *multiple bridge interface, bridging firewalling*.
5. *Data Rate Management* : QoS berbasis HTB dengan penggunaan *burst*, PCQ, RED, SFQ, FIFO *queue*, CIR, MIR, *limit* antar *peer to peer*.
6. DHCP : Mendukung DHCP tiap antarmuka, DHCP *Relay*, DHCP *Client*, *multiple network* DHCP, *static and dynamic* DHCP *leases*.
7. *Firewall* dan NAT : Mendukung pemfilteran koneksi *peer to peer*, *source* NAT dan *destination* NAT. Mampu memfilter berdasarkan MAC, IP *address*, *range port*, protokol IP, pemilihan opsi protokol seperti ICMP, TCP *Flags* dan MSS.
8. *Hotspot* : Hotspot *gateway* dengan otentikasi RADIUS. Mendukung *limit data rate*, SSL , HTTPS.
9. IPSec : Protokol AH dan ESP untuk IPSec, MODP *Diffie-Hellmann groups* 1, 2, 5; MD5 dan algoritma SHA1 *hashing*; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; *Perfect Forwarding Secresy* (PFS) MODP groups 1, 2, 5.
10. ISDN : Mendukung ISDN *dial-in/dial-out*. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, *Radius*. Mendukung 128K *bundle*, *Cisco* HDLC, x751, x75ui, x75bui *line* protokol.
11. M3P : MikroTik Protokol Paket Packer untuk wireless *links* dan *ethernet.*
12. MNDP : MikroTik *Discovery Neighbour Protokol*, juga mendukung *Cisco Discovery Protokol* (CDP).
13. *Monitoring / Accounting* : Laporan *Traffic* IP, *log*, statistik *graph* yang dapat diakses melalui HTTP.

14. NTP : *Network Time Protokol* untuk server dan *clients*; sinkronisasi menggunakan *system* GPS.
15. *Poin to Point Tunneling Protocol* : PPTP, PPPoE dan L2TP *Access Consentrator*; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit *data rate*.
16. *Proxy* : *Cache* untuk FTP dan HTTP *proxy server*, HTTPS *proxy*; *transparent proxy* untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung *parent proxy*; *static* DNS.
17. *Routing* : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
18. SDSL : Mendukung *Single Line* DSL; mode pemutusan jalur koneksi dan jaringan.
19. *Simple Tunnel* : Tunnel IPIP dan EoIP (*Ethernet over* IP).
20. SNMP : *Simple Network Monitoring Protocol mode akses read-only*.
21. *Synchronous* : 35, V.24, E1/T1, X21, DS3 (T3) *media ttypes*; *sync*-PPP, *Cisco* HDLC; *Frame Relay line protokol*; ANSI-617d (ANDI atau *annex* D) dan Q933a (CCITT atau annex A); *Frame Relay jenis* LMI.
22. *Tool* : *Ping, Traceroute; bandwidth test; ping flood; telnet*; SSH; *packet sniffer*; *Dinamic* DNS *update*.
23. UPnP : Mendukung antarmuka *Universal Plug and Play*.
24. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan *ethernet dan wireless*; *multiple* VLAN; VLAN *bridging*.
25. VoIP : Mendukung aplikasi *voice over* IP.
26. VRRP : Mendukung *Virtual Router Redudant Protocol*.
27. *WinBox* : Aplikasi mode GUI untuk *remote* dan mengkonfigurasi MikroTik RouterOS. (Hendriyanto Febrian 2011)

2.4 Definisi dan Komponen MPLS

Multiprotocol Label Switching (MPLS) adalah teknologi penyampaian paket pada jaringan backbone (jaringan utama) berkecepatan tinggi yang menggabungkan beberapa kelebihan dari sistem komunikasi *circuit-switched* dan *packet-switched* yang melahirkan teknologi yang lebih baik dari keduanya (Fathurrahmad and Yusuf 2019). MPLS menggabungkan teknologi *switching* di *layer* 2 dan teknologi *routing*

di *layer* 3 sehingga menjadi solusi jaringan dalam menyelesaikan masalah kecepatan, *scalability*, QoS (*Quality of Service*), dan rekayasa trafik (Rahmadita and Hadi 2010). MPLS terdiri dari beberapa komponen, diantaranya yaitu :

1. *Label Switched Path* (LSP)

   Merupakan jalur yang melalui satu atau serangkaian *Label Switching Router* (LSR) dimana paket diteruskan oleh label *swapping* dari satu MPLS *noode* ke MPLS *noode* yang lain.

2. *Label Switching Router* (LSR)

   Merupakan sebuah router dalam jaringan MPLS yang berperan dalam menetapkan *Label Switched Path* (LSP) dengan menggunakan teknik label *swapping* dengan kecepatan yang telah ditetapkan. LSR dapat dibagi menjadi dua, yaitu:

   a. *Ingress* LSR : berfungsi mengatur trafik saat paket memasuki jaringan MPLS.
   b. *Egress* LSR : berfungsi untuk mengatur trafik saat paket meninggalkan jaringan MPLS menuju ke LER

3. *Label Edge Router* (LER)

   LER merupakan peralatan yang beroperasi pada jaringan akses dan jaringan MPLS. LER mempunyai kemampuan untuk dihubungkan dengan jaringan yang tidak sama atau sejenis, seperti *frame relay*, ATM dan *Ethernet*, dan meneruskan *trafik* tersebut ke jaringan MPLS setelah pembentukan LSP, dengan menggunakan label *signalling protocol* pada *ingress* LSR dan mendistribusikan trafik kembali menuju jaringan akses pada bagian *egress* LSR

4. *Forward Equivalence Class* (FEC)

   Merupakan representasi dari beberapa paket data yang diklasifikasi berdasarkan kebutuhan *resource* yang sama didalam proses pertukaran data.

5. *Label*

   Merupakan deretan bit informasi yang ditambahkan pada *header* suatu paket data dalam jaringan MPLS. MPLS atau MPLS *header* ini terletk diantara *header layer 2* dan *header layer* 3.

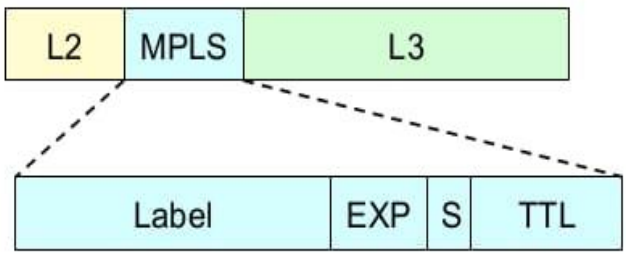
6. *Label Distribution Protocol* (LDP)

   Merupakan protokol yang berfungsi untuk mendistribusikan informasi yang terdapat dalam label disetiap LSR pada jaringan MPLS. Protokol ini digunakan untuk memetakan *Forward Equivalence Class* (FEC) kedalam tabel untuk selanjutnya akan dipakai dalam menentukan *Label Switched Path* (LSP). LDP message dapat dikelompokkan menjadi:

   a. *Discovery Messages*, yaitu pesan yang memberitahukan dan memelihara hubungan dengan LSR yang baru tersambung ke jaringan MPLS.
   b. *Session Messages*, yaitu pesan untuk membangun, memelihara dan mengakhiri sesi antara titik LDP.
   c. *Advertisement Messages*, yaitu pesan untuk membuat, mengubah dan menghapus pemetaan label pada jaringan MPLS.
   d. *Notification Messages*, yaitu pesan yang menyediakan informasi bantuan dan sinyal informasi jika terjadi error.

2.5 *Header* MPLS

MPLS memiliki *header* yang kemudian disebut dengan *hedaer* MPLS. *Header* MPLS terdiri dari 32 bit, dimana 32 bit tersebut terbagi kedalam 4 bagian, yakni: 20 bit digunakan untuk label, 3 bit digunakan untuk fungsi *experimental*, 1 bit digunakan untuk fungsi *stack* dan 8 bit digunakan untuk fungsi *time-to-live* (TTL) (Hanifia 2019). *Header* MPLS dapat dilihat pada Gambar 2.1 berikut.



Gambar 2.1 *Header* MPLS

Gambar diatas merupakan gambar *Header* MPLS paket dengan rincian sebagai berikut :

a. *Label Value* (LABEL)

   Merupakan *field* yang terdiri dari 20 bit yang merupakan nilai dari label tersebut. Nilai label tersebut contohnya alamat IP, besar data, jenis data dan lain-lain.

b. *Experimental Use* (EXP)

   Secara teknis *field* ini digunakan untuk keperluan eksperimen yaitu untuk menunjukkan antrian data yang masuk dan penjadwalan pengiriman paket. EXP terdiri dari 2 bit.

c. *Bottom of Stack* (STACK)

   Sebuah paket memungkinkan menggunakan lebih dari satu label. *Field* ini digunakan untuk mengetahui label *stack* yang paling bawah. Label yang paling bawah dalam *stack* memiliki nilai bit 1 sedangkan yang lain diberi nilai bit 0. Hal ini sangat diperlukan pada proses label *stacking*.

d. *Time-to-Live* (TTL)

   Field ini biasanya merupakan hasil salinan dari IP TTL header yang membantu dalam proses pendeteksian dan penghentian *looping* dari paket MPLS.

2.6 *Virtual Private LAN Service* (VPLS)

Virtual Private LAN Service atau disingkat VPLS merupakan *multipoint* VPN layer 2 yang menyediakan sebuah mekanisme yang memberikan kemampuan TLS (*Transparent LAN Service*) di seluruh jaringan IP atau MPLS (Adam Hudaya and Sulistyo 2018). Semua klien instans VPLS dapat terlihat berada di LAN yang sama meskipun terpisah secara geografis. VPLS menggunakan koneksi *Ethernet* untuk kliennya.

Jaringan VPLS terdiri dari *Customer Edge* (CE), *Provider Edge* (PE), dan jaringan MPLS sebagai *core network*-nya. *Customer Edge* (CE) merupakan sebuah *router* atau *switch* yang terletak pada sisi *client*, dapat dimiliki maupun di-*manage* oleh *service provider*. Paket dari client akan dikirimkan melalui *router* CE dan akan melalui router *Provider Edge* (PE) dan melewati jaringan MPLS sebagai *Core*

Network-nya secara transparan. Selanjutnya paket akan disampaikan lagi menuju *router* PE lainnya dan disampaikan juga ke *router* CE lainnya.

2.7 Routing

Routing adalah proses dimana suatu item dapat sampai ke tujuan dari satu lokasi ke lokasi lain. Beberapa contoh item yang dapat di-routing : *mail*, telepon *call*, dan data. Di dalam jaringan, Router adalah perangkat yang digunakan untuk melakukan routing trafik (Nurdiansyah et al. 2020).

Konsep dasar routing ialah bahwa dalam jaringan WAN kita sering mengenal yang namanya TCP/IP (*Transmission Control Protocol/ Internet Protocol*) sebagai alamat sehingga pengiriman paket data dapat sampai ke alamat yang dituju (host tujuan). TCP/IP membagi tugas masing-masing mulai dari penerimaan paket data sampai pengiriman paket data dalam sistem sehingga jika terjadi permasalahan dalam pengiriman paket data dapat dipecahkan dengan baik. Berdasarkan pengiriman paket data routing dibedakan menjadi routing langsung dan routing tidak langsung.

2.8 *Open Shortest Path Firs*t (OSPF)

OSPF (*Open Shortest Path First*) adalah sebuah protokol routing yang dikembangkan untuk jaringan IP oleh Internet Engineering Task Force (IETF) (Irwansyah 2017). OSPF adalah jenis protokol routing IGRP (*Interior Gateway Routing Protocol*) yang hanya dapat bekerja melalui jaringan internal organisasi atau perusahaan. Jaringan internal maksudnya adalah jaringan di mana *client* masih memiliki hak untuk menggunakan, mengatur, dan memodifikasinya, atau dengan kata lain, masih memiliki hak administrasi terhadap jaringan tersebut. Suatu jaringan dapat diklasifikasikan sebagai jaringan eksternal jika tidak memiliki izin untuk mengakses dan mengontrolnya.

OSPF merupakan routing protokol yang berstandar terbuka. Maksudnya adalah routing protokol ini bukan ciptaan dari vendor manapun. Dengan demikian, siapapun dapat menggunakannya, perangkat manapun dapat kompatibel dengannya, dan di manapun routing protokol ini dapat diimplementasikan. OSPF merupakan routing protokol yang menggunakan konsep hirarki routing, artinya

OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan area.

OSPF juga merupakan suatu protokol *routing link state* yang diterapkan pada suatu *intra autonomus syste*m. Algoritma yang digunakan pada routing OSPF adalah metode *link state*. OSPF merupakan protokol routing dengan menggunakan *link-state* yang dibentuk untuk bekerja secara tepat berdasarkan pengiriman *update* informasi rute. Algoritma OSPF biasaya menggunakan metode *link state* untuk mengkalkulasi *shortest path* pada setiap *destination node*. Pada protokol routing *link state* mempunyai informasi yang lengkap dan akurat tentang *network* yang akan dilalui di semua router.

Router menjalankan atau melakukan *broadcast* mengenai informasi routing kepada setiap router dalam suatu *Autonomus System*. Jika terjadi perubahan dalam informasi routing maka router mengimkan broadcast ke semua router. Sebuah router akan mengirimkan *broadcast link-state* ke setiap router lainnya jika terdapat perubahan informasi pada *network* seperti perubahan cost dan status network yang berubah (Amuda, Mulya, and Kurniadi 2021). OSPF memiliki beberapa kelebihan, yakni sebagai berikut:

1. OSPF merupakan protokol standar terbuka.
2. OPSF selalu menentukan rute atau jalur tercepat.
3. Jika ada perubahan dalam jaringan, maka database diupdate dengan cepat.
4. Menggunakan bandwith yang kecil untuk mengirimkan paket data.
5. Mendukung banyak rute atau jalur untuk sampai ke network tujuan.
6. OSPF didasarkan pada cost interface.
7. Support atau mendukung Variable Length Subnet Mask (VLSM).

2.9 Virtual Machine

Virtual Machine merupakan solusi untuk mengurangi jumlah komputer server yang di gunakan dalam suatu perusahaan. Pada penelitian kali ini, penulis menggunakan *VirtualBox* sebagai *Virtual Machine*. *Oracle VM VirtualBox* adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama. *VirtualBox* berfungsi untuk melakukan virtualisasi sistem operasi. *VirtualBox* juga dapat digunakan untuk membuat virtualisasi jaringan komputer sederhana (Anam et al. 2020).

2.10 *Graphical Network Simulator 3* (GNS3)

Graphical Network Simulator 3 (GNS3) adalah sebuah program *graphical network simulator* atau simulasi jaringan grafis untuk mensimulasikan topologi jaringan dengan lebih kompleks dibandingkan dengan simulator lainnya. Program ini dapat dijalankan pada *operating system*, seperti Windows maupun Linux (Juliantara Putra, Sudiarta, and Arsa Suyadnya 2017). Pada GNS3 memungkinkan simulasi jaringan yang komplek, karena menggunakan operating system asli dari perangkat jaringan, sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi router langsung. GNS3 adalah alat pelengkap yang sangat baik untuk laboratorium nyata bagi *network engineer*, administrator dan orang-orang yang ingin belajar membangun jaringan.

Fitur utama dari GNS3 adalah :

1) Desain kualitas tinggi dan topologi jaringan yang kompleks.
2) Mendukung banyak platform, tidak terbatas hanya satu platform saja.
3) Simulasi *Ethernet* sederhana, ATM dan *Frame Relay switch*.
4) Koneksi jaringan simulasi ke dunia nyata
5) Packet capture menggunakan Wireshark.

2.11 Winbox

WinBox adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke server *MikroTik* dalam mode GUI. Jika untuk mengkonfigurasi *MikroTik* dalam text mode melalui PC itu sendiri, maka untuk mode GUI yang menggunakan *WinBox* ini dapat melakukan konfigurasi *MikroTik* melalui komputer *client* (Moek, Atok, and Mige 2019). Kelebihan dari *WinBox* ini adalah kemudahan dalam melakukan *remote* karena berbasis GUI.

2.12 Wireshark

Wireshark banyak digunakan dalam memecahkan *troubleshooting* dijaringan untuk memeriksa keamanan jaringan, men-*debug* implementasi protocol jaringan dalam *software* mereka, melakukan *debugging* implementasi paket *protocol* dan banyak juga digunakan untuk *sniffer* atau mengendus data-data privasi dijaringan (Diansyah et al. 2015)s. Wireshark ini diibaratkan sebagai media atau tool yang dapat dipakai oleh user untuk penggunaannya, apakah untuk kebaikan atau

kejahatan. Hal ini karena wireshark dapat digunakan untuk mencari informasi yang sensitif yang berkeliaran pada jaringan, contoh nya kata sandi, cookie dan lain sebagainya.

Wireshark dapat menganalisis paket data secara *real time*. Artinya aplikasi wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah ditentukan oleh user sebelumnya. Wireshark dapat menganalisa paket data secara *real time*, artinya aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya.

2.13 Parameter *Quality of Service* (QOS)

Ada beberapa parameter pengukuran untuk *Quality of Service* (QoS) pada sebuah jaringan. Parameter dalam *Quality of Service* (QoS) memiliki sebuah standar yang sudah ada. Berikut adalah parameter yang dapat dilakukan untuk pengujian QoS (Nugita 2022), diantaranya :

a. *Throughput*

Throughput adalah kecepatan pengiriman data, dengan mengamati jumlah data yang dikirim antar client dengan selang waktu ketika data dikirim hingga akhirnya diterima. Pengukuran *throughput* dapat dilihat pada Tabel 2.1 berikut.

Tabel 2.1 Kategori *Throughput*

Kategori *Throughput*	***Throughput* (bps)**
Sangat Bagus	100
Bagus	75
Sedang	50
Buruk	<25

Rumus perhitungan nilai *throughput* :

$$\textit{Throughput} = \frac{\text{Jumlah } \textit{Bytes}}{\textit{Time Span}} \quad \text{..... (2.1)}$$

b. *Delay*

Delay merupakan waktu jarak tempuh suatu data ketika data dikirimkan dari pengirim menuju ke penerima.. Pengukuran *delay* dapat dilihat pada Tabel 2.2 berikut.

Tabel 2.2 Kategori *Delay*

Kategori delay	***Delay***
Sangat Bagus	< 150 ms
Bagus	150 ms s/d 300 ms
Sedang	300 ms s/d 450 ms
Buruk	> 450 ms

Rumus perhitungan nilai *delay* :

$$Delay = \frac{\text{Total } Delay}{\text{Total Paket yang Diterima}} \quad (2.2)$$

c. *Jitter*

Jitter merupakan *delay* yang menumpuk, dikarenakan adanya antrean sewaktu data diolah yang biasa terjadi di dalam perangkat router dan switch.. Pengukuran *jitter* dapat dilihat pada Tabel 2.3 berikut.

Tabel 2.3 Kategori *Jitter*

Kategori *Jitter*	***Jitter***
Sangat Bagus	0 ms
Bagus	75 ms
Sedang	125 ms
Buruk	225 ms

Rumus perhitungan nilai *jitter* :

$$Jitter = \frac{\text{Total Variasi } Delay}{\text{Total Paket yang Diterima}} \quad (2.3)$$

d. Packet Loss

Packet Loss merupakan paket data yang gagal mencapai tujuan akhir saat paket data dikirimkan. Pengukuran *Packet Loss* dapat dilihat pada Tabel 2.4 berikut.

Tabel 2.4 Kategori *Packet Loss*

Kategori *Packet Loss*	***Packet Loss***
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Buruk	25%

Rumus perhitungan nilai *packet loss* :

$$\textit{Packet Loss} = \frac{\text{Paket Dikirim} - \text{Paket Diterima}}{\text{Paket Dikirim}} \times 100 \quad \text{..... (2.4)}$$