

BAB II

TINJAUAN PUSTAKA

2.1. Penelitian Sebelumnya

Penelitian sebelumnya berjudul “Analisis Performansi *Dynamic Multipoint Virtual Private Network* Pada Routing Protokol BGP Dengan FRRouting”. Pada penelitian ini menggunakan router *open source* FRRouting, namun Pada penelitian ini melakukan analisis *Dynamic Multipoint Virtual Private Network* (DMVPN) pada *protokol BGP* dan menggunakan *throughput, jitter, delay, packet loss* sebagai parameter untuk melakukan analisis performansi. Penelitian ini memiliki hasil *throughput* 3400 – 3500, *delay* 0,4 – 1 detik, *jitter* 0,3 – 0,4 ms dan *packet loss* 0% yang dimana *throughput, jitter,* dan *packet loss* dalam standar TIPHON termasuk baik namun memiliki *delay* yang buruk[5].

Pada penelitian milik Mardianto M yang berjudul “Analisis *Quality Of Service* pada jaringan VPN dan MPLS VPN menggunakan GNS3”. Melakukan analisis terhadap jaringan VPN dan MPLS VPN yang di simulatkan menggunakan GNS3. Pada penelitian kali ini juga menggunakan standarisasi TIPHON namun dalam penelitian ini hanya menggunakan tiga parameter saja yaitu *throughput, packet loss,* dan *delay* tidak ada untuk pengujian *jitter* pada penelitian ini, dan hasil dari penelitian ini menunjukkan hasil *delay* dan *packet loss* sama bagusnya, tetapi untuk *throughput* MPLS VPN lebih stabil dibandingkan dengan VPN[8].

Penelitian selanjutnya melakukan analisa terhadap video streaming menggunakan jaringan MPLS dan VPLS yang berjudul “Analisis QoS Streaming Video Jaringan MPLS Dan VPLS”. Pada penelitian ini menggunakan router dari cisco 2691 dan menggunakan GNS3 untuk melakukan simulasi dan menggunakan wireshark untuk memantau lalu lintas dari jaringan, dan melakukan analisa dengan parameter *throughput, delay,* dan *packet loss*. Pada penelitian ini menggunakan tiga kualitas video yang berbeda mulai dari 360p, 480p, 720p jadi nilai dari parameter didapat

berdasarkan kualitas video. Hasil dari pengujian tersebut pada throughput video 360p VPLS mendapatkan hasil yang lebih tinggi dari MPLS, namun pada pengujian video 480p, dan 720p MPLS mendapatkan hasil yang lebih tinggi dari VPLS. Sehingga disimpulkan pada penelitian ini bahwa throughput pada VPLS memiliki hasil yang kurang stabil, pada pengujian delay pada penelitian ini MPLS mendapatkan hasil yang lebih sedikit dari VPLS. Namun kestabilan terlihat kurang baik terlihat pada pengujian video dengan kualitas 480p MPLS mengalami kenaikan yang cukup signifikan dan turun lagi pada pengujian video dengan kualitas 720p, sedangkan untuk VPLS walaupun memiliki delay yang cukup besar namun stabil tidak mengalami kenaikan yang signifikan seperti MPLS. Untuk pengujian packet loss keduanya memiliki hasil yang sama yaitu tidak memiliki packet loss[9].

Pada penelitian milik Gunawan M yang berjudul "Evaluasi Performa QOS MPLS L3VPN Dengan MPLS L3VPN *OVER GENERIC ROUTING ENCAPSULATION (GRE) Tunneling*". Pada penelitian kali ini melakukan evaluasi performa terhadap MPLSL3VPN dengan MPLSL3VPN *OVER GENERIC ROUTING ENCAPSULATION (GRE)*. Evaluasi performa pada penelitian ini menggunakan parameter dari *Quality of Server* dan menggunakan GNS3 untuk melakukan simulasi, dan pada parameter ping *response, convergence time, jitter* tidak menunjukkan hasil yang berbeda, namun pada pengujian throughput MPLSL3VPN menunjukkan hasil yang lebih baik. Pada *packet loss* MPLSL3VPN *OVER GRE* tunneling menunjukkan hasil yang lebih baik[10].

Penelitian ini berjudul "Evaluasi Kinerja Jaringan DMVPN phase3, MPLS L3VPN, dan VPLS Terhadap Layanan Video Streaming dan *File Transfer*". Pada penelitian ini membandingkan tiga jaringan yang berbeda dimana menggunakan protokol OSPF, BGP, dan EIGRP. Pada pengujian ini menggunakan parameter *throughput, delay, dan packet loss*, parameter tersebut dilakukan untuk melakukan pengujian berupa video streaming dan *file transfer*. Hasil pengujian pada penelitian ini MPLS L3 VPN dan DMVPN memiliki hasil yang baik dalam pengujian *file transfer* sedangkan VPLS dan

MPLS memiliki nilai yang baik pada video *streaming* baik pada *file* .mp4 maupun .mkv dibandingkan dengan DMVPN[11].

Dari beberapa penelitian diatas sudah ada yang menggunakan FRR dan sudah ada yang membuat jaringan dengan menggunakan MPLS L3 VPN yang memiliki hasil baik namun belum ada yang melakukan pengujian MPLS L3 VPN pada FRR. Pada penelitian [5] menunjukan performa dari FRR yang tergolong baik dalam menangani tabel perutean. Namun pada penelitian ini menggunakan DMVPN untuk membangun jaringan nya. Dan pada penelitian [8] menunjukan kestabilan penerusan paket pada MPLS VPN namun pada penelitian ini tidak menjelaskan perangkat router yang digunakan. Dari hasil penelitian tersebut menunjukkan bahwa performa dari FRR dan MPLS VPN memiliki hasil yang bagus. Dan dalam penelitian ini menggunakan router FRR dan MPLS L3 VPN untuk membangun sebuah jaringan. Karena FRR bersifat *opensource* tentunya bisa menjadi kelebihan karena bisa mengurangi penggunaan budget pada pembuatan jaringan namun memiliki performa yang baik dalam meneruskan paket data ke tujuannya.

Tabel 2. 1 Tabel Penelitian Sebelumnya

No	Judul/paper	Metode	Objek	Kesimpulan	Saran	Tahun
1	Analisis Performansi Dynamic Multipoint Virtual Private Network Pada Routing Protokol BGP Dengan FRRouting	<i>Research and Development</i>	DMVPN pada routing Protokol BGP menggunakan FRRouting	analisis performansi penelitian ini memiliki hasil throughput 3400 – 3500, delay 0,4 – 1 detik, jitter 0,3 – 0,4 ms dan packet loss 0% yang dimana throughput, jitter, dan packet loss dalam standar TIPHON termasuk baik namun memiliki delay yang buruk		2021
2	<i>Analisis Quality Of Service pada jaringan VPN dan MPLS VPN menggunakan GNS3</i>	<i>Research and Development</i>	VPN dan MPLSVPN	hasil dari penelitian ini menunjukkan hasil delay dan packet loss sama bagusnya, tetapi untuk <i>throughput</i> MPLS VPN lebih stabil dibandingkan dengan VPN	Tidak ada nya parameter jitter pada pengujian, yang menyebabkan kurang maksimal dalam hasil karena jitter adalah variasi delay yang menghitung delay pertama dan delay selanjutnya, dengan jitter kita bisa mengetahui stabil atau tidaknya koneksi internet.	2019
3	Evaluasi Performa QOS MPLS L3VPN Dengan MPLS L3VPN OVER GENERIC ROUTING	<i>Research and Development</i>	JMPLS L3 VPN dan MPLS L3 VPN Over <i>GENERIC ROUTING ENCAPSULATION Tunneling</i>	dan pada parameter ping response, convergence time, jitter tidak menunjukan hasil yang berbeda namun pada pengujian throughput MPLSL3VPN menunjukan hasil yang lebih baik		2018

No	Judul/paper	Metode	Objek	Kesimpulan	Saran	Tahun
	ENCAPSULATION (GRE) Tunneling			namun pada packet loss MPLSL3VPN OVER GRE tunneling menunjukkan hasil yang lebih baik		
4	Evaluasi Kinerja Jaringan DMVPN phase3, MPLS L3VPN, dan VPLS Terhadap Layanan Video Streaming dan File Transfer	Kualitatif	Pengujian video streaming dan file transfer dengan DMVPN, MPLSL3VPN, VPLS	hasil pengujian pada penelitian ini MPLS L3 VPN dan DMVPN memiliki hasil yang baik dalam pengujian file transfer sedangkan VPLS dan MPLS memiliki nilai yang baik pada video streaming baik pada file .mp4 maupun .mkv dibandingkan dengan DMVPN		2019
5	Analisis QoS Streaming Video Jaringan MPLS Dan VPLS	Kualitatif	Pengujian kualitas video streaming dengan MPLS dan VPLS	Pada pengujian ini VPLS memiliki hasil yang lebih stabil dari MPLS dari segi throughput dalam kualitas video 360p. Namun pada kualitas 480p, dan 720p MPLS mendapat nilai yang lebih baik. Dan delay dari MPLS juga menunjukkan nilai yang baik namun dari tiga pengujian video delay pada MPLS memiliki nilai yang kurang stabil		2019

2.2. Dasar Teori

1.2.1. WAN (*Wide Area Network*)



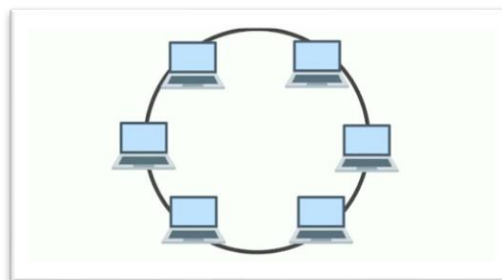
Gambar 2. 1 WAN (*Wide Area Network*)[12]

Wide Area Network adalah jaringan komputer yang mencakup area yang besar, yang berguna untuk memudahkan dalam berkomunikasi baik antar negara maupun benua. Sebagai contoh adalah jaringan yang menghubungkan suatu wilayah atau suatu negara dengan negara lainnya sehingga jaringan lokal suatu wilayah dengan jaringan lokal wilayah lain dapat terhubung[12].

1.2.2. Topologi Jaringan

Topologi merupakan suatu tatanan untuk menghubungkan beberapa komputer atau perangkat-perangkat jaringan yang digunakan menjadi suatu jaringan yang saling terhubung. Terdapat bermacam-macam jenis topologi yang digunakan pada jaringan internet saat ini yaitu topologi *ring*, *tree*, *star*, *mesh*, *bus*[13].

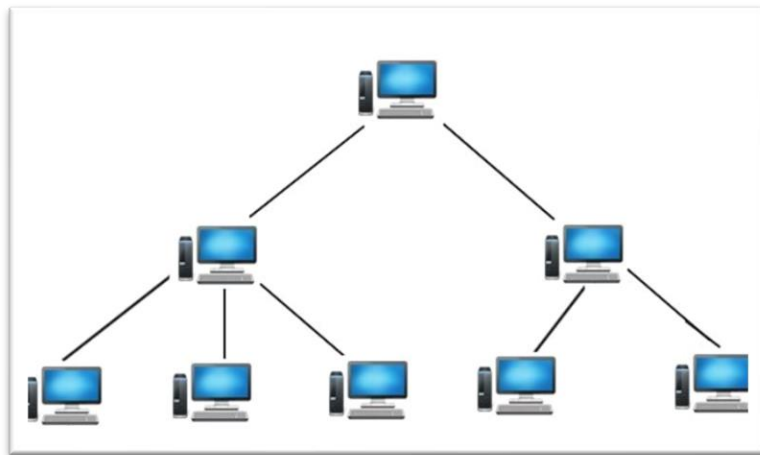
1.2.2.1. Topologi *ring*.



Gambar 2. 2 Topologi Ring

Pada topologi ring, setiap perangkat terhubung dengan dua perangkat lainnya membentuk bentuk cincin. Data bergerak melalui jaringan dari satu perangkat ke perangkat berikutnya hingga mencapai tujuan. Topologi ini sederhana dan mudah diimplementasikan, tetapi kerentanannya tinggi karena gangguan pada satu perangkat dapat mengganggu seluruh jaringan.

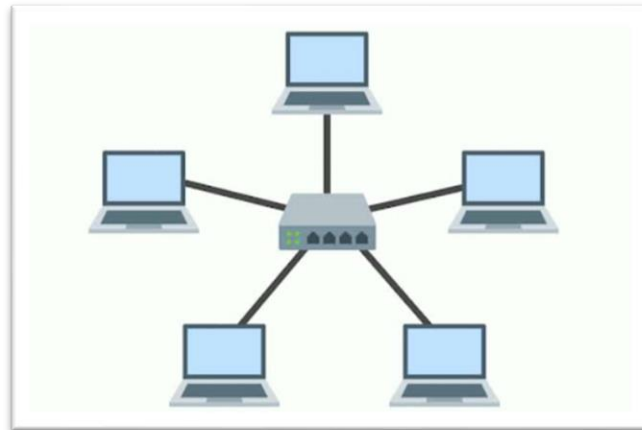
1.2.2.2. Topologi *tree*



Gambar 2. 3 Topologi tree

Topologi pohon memiliki struktur hierarkis seperti pohon dengan akar sebagai node pusat dan cabang-cabangnya mewakili perangkat dalam jaringan. Topologi ini umumnya digunakan dalam jaringan besar yang melibatkan banyak perangkat dan departemen. Hierarki memudahkan manajemen, tetapi kelemahannya adalah jika node pusat gagal, seluruh bagian jaringan yang terhubung dengannya dapat terpengaruh.

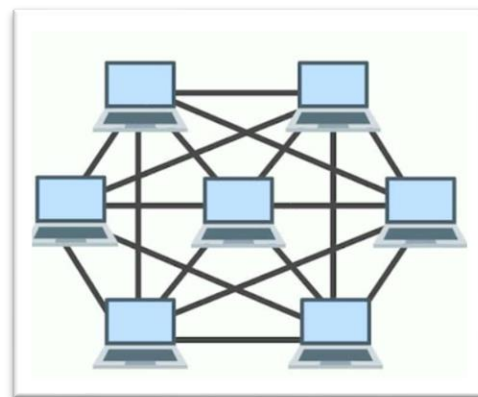
1.2.2.3. Topologi *star*



Gambar 2. 4 Topologi Star

Topologi star memiliki pusat atau simpul sentral yang berfungsi sebagai hub atau switch yang menghubungkan semua perangkat dalam jaringan. Setiap perangkat terhubung langsung ke pusat, sehingga jika satu koneksi terputus, hanya perangkat yang terkena dampak, dan jaringan lain tetap berfungsi. Topologi star memudahkan manajemen dan deteksi masalah jaringan, tetapi jika pusat mengalami masalah, seluruh jaringan dapat terpengaruh.

1.2.2.4. Topologi *mesh*

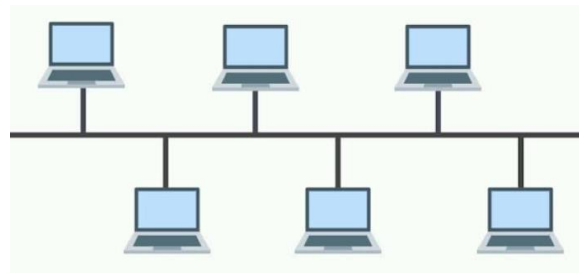


Gambar 2. 5 Topologi mesh

Topologi mesh melibatkan setiap perangkat terhubung langsung ke semua perangkat lain dalam jaringan. Jumlah koneksi dalam topologi ini

meningkat secara eksponensial dengan penambahan perangkat, sehingga topologi mesh sering digunakan dalam jaringan kecil atau pada saluran komunikasi khusus. Topologi mesh memberikan redundansi yang tinggi, memungkinkan komunikasi yang andal, tetapi biaya dan kompleksitas pemasangan dan pemeliharaan jaringan dapat menjadi tantangan.

1.2.2.5. Topologi Bus



Gambar 2. 6 Topologi Bus

Dalam topologi bus, semua perangkat terhubung ke satu jalur pusat (bus) yang berfungsi sebagai saluran tunggal untuk komunikasi data. Data yang dikirimkan oleh satu perangkat dapat diakses oleh semua perangkat lain yang terhubung ke bus. Keuntungan dari topologi ini adalah mudah dalam instalasi dan biaya rendah, tetapi kerugiannya adalah jika ada gangguan pada jalur pusat, seluruh jaringan dapat terpengaruh [14].

1.2.3. Routing Protokol

Protokol *routing* adalah aturan untuk bertukar informasi routing yang membuat tabel *routing* untuk memperjelas pengalamatan dalam paket data yang dikirim, dan juga mencari rute terpendek untuk mengantarkan paket data ke alamat tujuan yang dituju. *Routing* bertanggung jawab untuk mengangkut data melalui beberapa jaringan dengan memilih jalur yang sesuai untuk perjalanan data. Algoritma routing menentukan pilihan jalur melalui beberapa jaringan, tergantung

pada metode yang digunakan untuk berbagi informasi eksternal, dimana algoritma adalah metode yang digunakan untuk memproses informasi internal.

1. *Distance vector*

Protokol *distance vector* memberitahu rentang lompatan hop ke jaringan tujuan (*the distance*) dan jalur di mana paket dapat mencapai jaringan tujuan (*vector*). algoritma *distance vector*, juga disebut sebagai algoritma Bellman-Ford, router dapat melewati *updates route* ke tetangga mereka pada interval rutin terjadwal, setiap tetangga kemudian mendapatkan nilai tujuannya sendiri dan menyalurkan ke tetangga terdekat dan meneruskan data perutean ke tetangga terdekat. Hasil akhir dari cara ini adalah tabel yang berisi kumpulan semua tujuan ke semua jaringan. sejumlah protokol yang termasuk sebagai *Distance Vector* adalah RIP dan BGP.*Link state*

2. *Link State*

routing dibentuk dengan cara mengumpulkan informasi tentang *interface, bandwidth, roundtrip*, dan faktor-faktor lainnya dari setiap router. Kemudian, informasi tersebut akan ditukar antar router dan nilai yang paling efisien akan dipilih dan dimasukkan ke dalam tabel *routing*. Untuk mengambil keputusan tersebut, digunakan algoritma *Shortest Path First* (SPF) yang mengatur informasi *Link State Advertisement* (LSA) sedemikian rupa sehingga membentuk jalur *routing*. Oleh karena itu, protokol OSPF menggunakan algoritma SPF

3. *Hybrid Protokol*

hybrid menggunakan aspek-aspek dari routing protokol jenis *distance-vector* dan routing protokol jenis *link-state* sebagai contoh adalah EIGRP[15].

1.2.4. OSPF

OSPF (Open Shortest Path First) adalah sebuah protokol routing jenis

link-state yang termasuk dalam kelas IGP (Interior Gateway Protocol). Protokol ini menggunakan algoritma Dijkstra untuk menghitung jalur terbaik ke jaringan dengan mempertimbangkan cost sebagai metrik. Dengan menggunakan algoritma Dijkstra OSPF dapat menemukan rute terpendek dalam melakukan routing. Algoritma Dijkstra bekerja secara incremental dari titik awal yang menyebar ke seluruh titik dalam graf. Pada setiap iterasi, algoritma akan memperbarui tabel jarak dengan mengambil tetangga terdekat dari titik yang dikunjungi, sehingga mencari jalur terpendek secara bertahap. OSPF mengadopsi konsep area dalam pengaturan jaringan. Saat ada perubahan dalam jaringan, OSPF akan segera mengirimkan pesan multicast ke semua host untuk memberitahu perubahan tersebut. mengirimkan informasi tabel routing yang telah berubah dan paket Hello setiap 10 detik[16].

1.2.5. BGP

BGP (Border Gateway Protocol) adalah sebuah protokol routing eksterior yang digunakan dalam jaringan komputer untuk mengatur pertukaran informasi routing antara sistem otonom (autonomous system/AS). AS adalah sekelompok jaringan yang diatur oleh satu otoritas administratif tunggal dan dapat mencakup beberapa jaringan lokal yang saling terhubung. Fungsi utama BGP adalah untuk membantu menentukan jalur terbaik bagi lalu lintas data di antara sistem otonom yang berbeda. Ketika lalu lintas data harus dikirimkan dari satu AS ke AS lainnya, BGP akan menginformasikan rute terbaik yang dapat digunakan untuk mencapai tujuan tersebut[3].

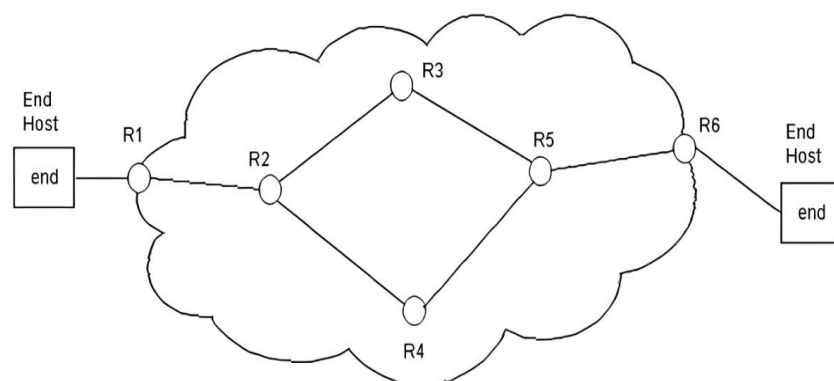
1.2.6. Performansi Jaringan

Merupakan hal penting dalam mengelola jaringan, karena memberikan informasi kepada operator untuk melakukan monitoring lalu lintas jaringan. Dengan hal ini membuat operator dapat mengetahui kendala dalam jaringan dan dapat diatasi sesuai dengan prosedur yang ada. Dengan melakukan pemantauan jaringan dapat mengetahui kualitas dari jaringan dan juga bisa meningkatkan kualitas jaringan sesuai dengan

kebutuhan dalam sebuah jaringan. Meningkatkan kualitas jaringan memberikan kepuasan bagi operator dan pengguna dalam menggunakan jaringan[17].

1.2.7. MPLS

MPLS, kepanjangan dari "*Multi Protocol Label Switch*", yang memungkinkan pengiriman data di jalur backbone dengan kecepatan tinggi. Konsep MPLS memadukan keuntungan dari teknik *switch circuit* dan *switch packet* untuk memberikan solusi yang lebih efisien. Dengan demikian MPLS dapat diartikan sebagai teknologi pengiriman data yang mengkombinasikan prinsip-prinsip dari teknik *switch circuit* dan *packet* untuk meningkatkan efisiensi dalam pengiriman data pada jaringan backbone. Setiap paket akan diberi label yang berisi catatan perutean untuk paket termasuk tujuan paket dan masalah paket mana yang harus ditambahkan terlebih dahulu. Informasi label ini diperoleh dari layer jaringan perutean, sehingga setiap paket hanya akan dianalisis satu kali melalui router tepi tempat paket pertama kali masuk ke jaringan. Metode ini akan mempercepat waktu perutean karena hanya membutuhkan satu dedikasi saja melalui router bagian atau yang biasa disebut *Label Switching Router (LSR)*. LSR atau label transfer *route* adalah sirkuit yang menghubungkan antar LSR. LSR primer dan penutup disebut sebagai *inngress* dan *egress* [15].

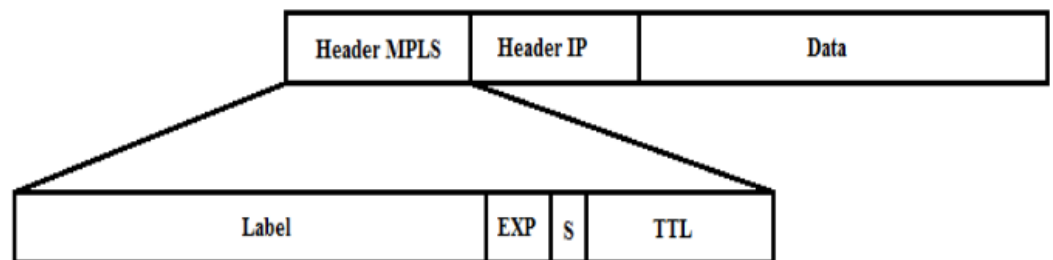


Gambar 2. 7 cara kerja mpls

R1 dan R6 pada Gambar 2.2 disebut *Edge* router, ditempatkan di

bagian depan perbatasan dari domain IP. R2, R3, R4 dan R5 disebut *Core Router*, tidak berhubungan langsung dengan dunia luar kecuali melalui Edge router, Edge router sebagai *Label-Edge-Router (LER)* dan *Core Router* sebagai *Label Switched-Router (LSR)*. LER mengkonversi paket IP ke paket MPLS dan sebaliknya. Ketika paket-paket tersebut masuk ke LER, konversi yang dilakukan adalah dari paket IP ke paket MPLS, dan ketika keluar dari LER, konversi dari paket MPLS ke paket IP.[18]

1.2.8. Paket MPLS



Gambar 2. 8 Pemetaan header pada MPLS[18]

MPLS bekerja dengan menambahkan *header* MPLS pada paket ip, yang terdiri dari 32 bit dan dibagi menjadi empat bagian yaitu 20 bit digunakan sebagai label, lalu 3 bit untuk eksperimental, 1 bit untuk fungsi *stack*, dan 8 bit untuk time-to-live(TTL). *Header* pada MPLS memiliki fungsi sebagai penghubung *header* layer 2 dengan layer 3, dan label pada MPLS merupakan identifikasi pada paket, dengan demikian MPLS melakukan enkapsulasi paket IP dengan menambahkan *header* MPLS pada paket tersebut. Gambar diatas merupakan gambar format MPLS *header* paket dengan beberapa rincian yaitu :

a. *Label Value (LABEL)*

Adalah *field* yang terdiri dari 20 bit merupakan nilai dari label yang mencakup informasi seperti alamat IP, ukuran data, jenis data, dan elemen lainnya.

b. *Experimental Use (EXP)*

Secara teknis bidang ini digunakan untuk keperluan

percobaan, yaitu menampilkan urutan data yang diterima serta mengatur pengiriman paket dan terdiri dari 2 bit

c. *Bottom of Stack (STACK)*

Dalam label *stacking* suatu paket dapat menggunakan beberapa label untuk mengetahui label stack terbawah. Label yang paling bawah pada stack diberi nilai bit 1, sementara label lainnya diberi nilai bit 0, hal ini berguna untuk melaksanakan 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[18].

1.2.9. VPN

VPN merupakan teknologi yang memungkinkan pengguna dapat terhubung dengan jaringan publik dan memanfaatkan untuk bergabung ke jaringan lokal[19]. VPN juga merupakan koneksi pribadi antara dua jaringan yang terhubung dengan internet yang merupakan jaringan publik. Dengan VPN juga pengguna dapat terhubung dengan jaringan VPN lainya melalui sebuah *tunnel virtual* antara dua node sehingga pengiriman data lebih aman[2].

1.2.10. MPLSVPN

MPLS VPN merupakan jenis jaringan yang memusatkan pada koneksi antara router PE (*Provider Edge*) dan router CE (*Customer Edge*). Router CE terhubung dengan router PE sehingga data yang dikirim di enkapsulasi dan dapat diteruskan ke router CE lainya dalam jaringan. Router CE akan memberitahukan rute VPN ke seluruh perangkat jaringan untuk memastikan konektivitas yang baik. MPLS VPN terdiri dari beberapa lokasi yang saling terhubung melalui jaringan inti penyedia MPLS, dan disetiap lokasi terdapat satu atau beberapa router CE yang terhubung ke satu atau beberapa PE.

Router PE menggunakan MP-BGP(*Border Gateway protocol Multiprotocol*) untuk berkomunikasi secara dinamis antara router PE. Selama alamat IP yang digunakan dalam jaringan *core* MPLS VPN harus eksklusif dan berbeda dengan alamat IP yang dimiliki oleh pelanggan VPN. Setiap router CE harus mampu untuk mengirim paket data ke router PE yang berhadapan langsung. Alamat IP yang ada pada router PE tidak boleh ada yang sama dengan alamat IP milik pelanggan VPN. MPLS VPN yang berbasis Peer Model, memiliki skalabilitas yang tinggi, mudah untuk dibangun, dan mudah untuk di manajemen dibandingkan VPN konvensional. MPLS VPN memisahkan lalu lintas jaringan dengan tabel routing yang unik, yang disebut VRF (*Virtual Routing Forwarding*) pada setiap jaringan VPN milik pelanggan. Sehingga setiap pelanggan pada sebuah VPN tidak akan bisa melihat lalu lintas jaringan diluar VPN nya. Pemisahan lalu lintas jaringan terjadi tanpa proses tunneling ataupun enkripsi, karena sudah dibangun langsung di dalam jaringan *service provider*[8].

1.2.11. Routerboard dan Router OS

Router OS adalah *system* operasi linux yang dirancang khusus untuk dijadikan sebagai router jaringan. Sementara routerboard merujuk pada perangkat keras yang digunakan untuk menjalankan Router OS, mikrotik merupakan merek resmi yang memasangkan Router OS pada routerboard. Beberapa fitur yang terdapat pada Router OS antara lain *firewall* dan *NAT*, *routing*, *tunneling*, *ipsec*, *web proxy*, *SNMP*, *tools*, serta beberapa fitur lainnya[20].

1.2.12. Free Range Routing

Free Range Routing (FRR) merupakan rangkaian perutean IP yang memiliki kinerja unggul, fitur yang komprehensif, serta bersifat terbuka, FRR mengaplikasikan semua protokol perutean dinamis seperti BGP, RIP, IS-IS, dan sejenisnya. FRR adalah sebuah perangkat dengan kinerja superior yang dapat dengan mudah mengelola tabel perutean internet secara penuh, dan sesuai digunakan pada beragam perangkat keras,

mulai dari SBC dengan harga terjangkau hingga router komersial. FRR aktif digunakan dalam produksi oleh banyak perusahaan, universitas penelitian, dan pemerintah [5].

1.2.13. Jaringan Komputer

Jaringan komputer adalah dua atau lebih komputer yang terkoneksi satu sama lain. Komputer dapat terhubung dengan menggunakan kabel atau kabel telepon, atau dapat juga terhubung lewat wireless menggunakan gelombang radio, lewat kabel fiber optik maupun, lewat sinyal infrared. Ketika komputer dapat berkomunikasi, mereka dapat bekerja-sama dengan berbagai macam cara. Bisa dengan cara membagi resources satu sama lain dan membagi beban kerja dari suatu pekerjaan atau bertukar pesan[10].

1.2.14. Iperf3

iperf3 adalah untuk menguji dan memeriksa bandwidth atau kecepatan jaringan antara dua perangkat yang terhubung dalam jaringan. Alat ini mampu menguji bandwidth secara maksimum. Iperf3 bekerja dengan cara mengirimkan paket data melalui jaringan dan mengukur berapa banyak data yang dapat dikirimkan dan diterima dalam periode waktu tertentu. Pengukuran ini membantu dalam memahami seberapa baik kinerja jaringan dan seberapa efisien data dapat dikirimkan di antara dua titik. Dan pengiriman data juga dapat bekerja pada protokol jaringan TCP(*transmission Control Protocol*) dan UDP(*User Datagram Protocol*)[21].

1.2.15. GNS3

GNS3, atau *Graphic Network Simulator Version3*, adalah perangkat lunak sumber terbuka (GNU GPL) yang memungkinkan simulasi jaringan dengan tingkat kompleksitas yang mendekati kondisi jaringan nyata, tanpa memerlukan perangkat keras jaringan khusus seperti router dan switch. GNS3 sendiri merupakan sebuah program simulasi jaringan berbasis grafis yang dapat mensimulasikan topologi jaringan yang kompleks dengan mudah dan cepat, melalui konsep “*plug and play*”

yang sederhana dibandingkan dengan simulator lainnya. GNS3 menyediakan antarmuka pengguna grafis yang memudahkan perancangan dan konfigurasi di dalam jaringan virtual, serta berjalan pada perangkat keras PC dan dapat digunakan diberbagai system operasi seperti Windows, Linux, Mac OS X. Dalam memberikan simulasi yang lengkap dan akurat, GNS3 berfungsi sebagai emulator untuk menjalankan system operasi yang sama seperti pada jaringan nyata [15].

1.2.16. Router

Istilah router pada dasarnya berasal dari Bahasa Inggris yaitu kata Route yang artinya trayek atau mengarahkan perjalanan melalui yang ditambahi dengan imbuhan -er yang maknanya pelaku. Sehingga, jika diartikan dari asal katanya, maka router dapat diartikan sebagai sebuah perangkat yang digunakan untuk mengarahkan sinyal pada jaringan komputer. router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. supaya suatu paket dapat mencapai tujuannya, diperlukan suatu peralatan untuk mengatur paket - paket tersebut agar mencapai tujuannya dengan jalan yang tersingkat. Untuk itu perlu adanya router yang fungsi utamanya adalah untuk menentukan jalur dan mengirimkan paket dari suatu jaringan ke jaringan lain. Agar router dapat mengetahui jalur mana yang terbaik untuk mengirimkan paket ke alamat yang dituju, router menggunakan peta atau tabel routing.

Pada dasarnya fungsi router hampir sama dengan fungsi switch yaitu sebagai perangkat penghubung dalam jaringan komputer. Perangkat router digunakan untuk menghubungkan satu jaringan komputer dengan jaringan komputer lainnya. Jenis - jenis router diantaranya sebagai berikut :

1. Router Aplikasi

Router aplikasi adalah perangkat lunak yang berfungsi untuk mengubah perangkat komputer biasa memiliki kemampuan seperti router. .

2. Router Hardware

Perangkat keras router merupakan suatu perangkat fisik yang mampu mengambil dan menyebarkan sinyal, Router hardware erring disebut hanya sebagai “router”. Berbeda dengan router aplikasi yang tidak berwujud fisik, router hardware memiliki bentuk fisik yang nyata seperti perangkat keras lainnya .

3. Router PC

Sebuah router PC adalah perangkat komputer pribadi yang telah dimodifikasi agar dapat berfungsi sebagai router yang mampu menyebarkan sinyal seperti halnya router biasa. Router PC dapat dibuat dengan menggunakan perangkat komputer berkapasitas rendah(dengan spesifikasi minimal Pentium dua, *hard drive* 10GB, dan ram 64MB). Untuk mengubah perangkat komputer menjadi router, diperlukan instalasi system operasi khusus router, seperti salah satunya adalah system operasi Mikrotik. Fungsi utama dari router adalah untuk mengirimkan data antara segmen jaringan yang memiliki alamat jaringan yang berbeda [3].

1.2.17. Quality of Service (QoS)

Quality of Service (QoS) adalah evaluasi kinerja dan kualitas jaringan yang digunakan untuk menjamin tingkat kualitas layanan yang beragam. Berbagai jenis layanan memiliki kebutuhan performansi yang berbeda-beda dalam jaringan komputer. Standar pengukuran performansi dalam jaringan dikenal sebagai TIPHON (*telecommunications and internet protocol harmonitiation over network*), yang mengklasifikasi berbagai aspek performansi dalam perhitungan yang spesifik. [18].

1. Delay

Delay adalah interval waktu yang diperlukan oleh informasi

untuk melakukan perjalanan dari titik asal ke titik tujuan. Tujuan utama dalam mengukur *delay* adalah untuk mengetahui berapa lama waktu yang dibutuhkan oleh satu paket data untuk mencapai tujuannya, mulai dari sumber hingga mencapai tujuan. Nilai *delay* yang sangat bagus menurut standar TIPHON adalah < 150 ms tabel menunjukkan nilai *Delay* menurut standar TIPHON: [22]

Tabel 2. 2 Tabel Delay (TIPHON)[23]

Category	Delay
<i>Best</i>	<150ms
<i>Good</i>	150-300ms
<i>Medium</i>	300-450ms
<i>Poor</i>	>450ms

Untuk memperoleh nilai *Delay* digunakan rumus berikut:

$$Delay = \frac{Total\ delay}{Total\ packet\ yang\ diterima} \quad [9] \quad 2.1$$

2. *Throughput*

Throughput merujuk pada jumlah data yang dikirim melalui sebuah jaringan dalam jangka waktu tertentu, dari satu titik jaringan ke titik jaringan lainnya. Pengukuran *throughput* bertujuan untuk memahami sejauh mana keandalan jaringan dalam mengirimkan paket data secara efisien hingga mencapai tujuan akhir. menurut standar TIPHON:[22]

Tabel 2. 3 Tabel Throughput (TIPHON)[24]

Category	Throughput
<i>Best</i>	100%
<i>Good</i>	75%
<i>Medium</i>	50%
<i>poor</i>	<25

Berikut merupakan rumus untuk mendapatkan *throughput* :

$$\textit{Throughput} = \frac{\textit{jumlah packet yang dikirim (bit)}}{\textit{lamanya waktu pengiriman}} \quad [5] \quad 2.2$$

3. *Jitter*

Jitter adalah fluktuasi delay yang disebabkan oleh perbedaan Panjang antrian saat pemrosesan data dan pengumpulan kembali paket data pada akhir pengiriman setelah kegagalan sebelumnya. *Jitter* merupakan tantangan umum pada jaringan berbasis koneksi tanpa koneksi atau *packet switch*, tujuan pengukuran *jitter* adalah untuk memahami stabilitas pengalihan data dalam suatu jaringan. Stabilitas dapat diamati dari variasi *delay* yang terjadi selama periode komunikasi di dalam jaringan Berdasarkan standar TIPHON nilai *jitter* yang sangat bagus adalah 0 s/d 75 ms. Tabel berikut menunjukkan nilai *Jitter* menurut standar TIPHON:[22]

Tabel 2. 4 TabelJitter (TIPHON)[23]

Category	jitter
<i>Perfect</i>	0ms
<i>Good</i>	75ms
<i>Medium</i>	125ms
<i>Poor</i>	252ms

Berikut merupakan rumus untuk menghitung *Jitter* :

$$\textit{Jitter} = \frac{\textit{total variasi delay}}{\textit{total packet yang diterima}} \quad [5] \quad 2.3$$

4. *Packet Loss*

Packet loss adalah sebuah metrik yang mengindikasikan keadaan dimana paket-paket data hilang dalam jaringan akibat adanya tumpang tindih (*collusion*) atau kepadatan (*congest*) Satuan yang digunakan untuk mengukur *packet loss* adalah dalam bentuk persentase (%). Tujuan utama dari pengukuran *packet loss* adalah untuk mengevaluasi metode yang digunakan dalam proses pengiriman data efektif atau tidak. Berdasarkan

standar TIPHON nilai packet loss yang sangat bagus adalah 0%. Tabel 4 menunjukkan nilai Packet Loss menurut standar TIPHON:[22]

Tabel 2. 5 Tabel Packet Loss (TIPHON) [23]

Category	Packet loss
<i>Perfect</i>	0% - 2%
<i>Good</i>	3% - 14%
<i>Medium</i>	15% - 24%
<i>Poor</i>	>25%

Berikut merupakan rumus untuk mendapatkan nilai packet loss:

$$Packet Loss = \frac{packet\ send - packet\ received}{packet\ send} \times 100\% \quad [5] \quad 2.4$$

Parameter yang paling penting dalam mengevaluasi keandalan jaringan komputer adalah nilai Qos yang diperoleh. Semakin tinggi nilai Qos, maka semakin handal jaringan komputer tersebut.[22].