BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Sebagai bagian dari penelitian ini, dilakukan tinjauan literatur terhadap delapan jurnal yang mencakup topik terkait. Adapun ringkasan dari jurnal terkait adalah sebagai berikut :

Pada penelitian yang berjudul "*QoS Analysis on OSPFv3 and RIPng Using GRE Tunneling on IPv6 Integrated IPv4 Network*" yang ditulis oleh Indra Warman dan Alex Fanozal. Penelitian ini menjelaskan cara melakukan *tunnel* IPv6 melalui jaringan IPv4 menggunakan *tunneling Generic Routing Encapsulation* (GRE). Protokol *routing* yang digunakan dalam penelitian ini adalah RIPng dan OSPFv3. Dalam pengujian penelitian tersebut menggunakan laptop sebagai *client*, kemudian *server*, dan enam unit *router*, dimana untuk laptop dan *client* menggunakan IPv6 dan terhubung melalui jaringan IPv4, kemudian untuk *router* terhubung dengan menggunakan protokol *routing* RIPng dan OSPFv3. Dari topologi tersebut dilakukan pengujian dengan tiga skenario yang berbeda dan dengan beban paket data yang berbeda. Pengujian QoS dilakukan dengan cara menangkap paket data dengan menggunakan *tools* wireshark dan dilakukan perhitungan untuk mendapatkan nilai rata-rata *delay* dan *paket loss*. Hasil penelitian ini didapatkan bahwa nilai QoS dengan menggunakan protokol *routing* RIPng dan OSPFv3 dalam GRE *Tunneling*, OSPFv3 lebih baik dibandingkan dengan RIPng dari *parameter delay* dan *paket loss*[8].

Penelitian sebelumnya yang berjudul "Analisis Perbandingan Kinerja Protokol *Routing* OSPF, RIP, EIGRP, dan IS-IS" yang ditulis oleh Pahlevi Muhammad, dkk. Penelitian tersebut bertujuan untuk membandingkan antara *routing* protocol OSPF, RIP, EIGRP, dam IS-IS pada jaringan IPv6. Pada penelitian tersebut untuk mengetahui perbandingan nilai QoS menggunakan *software Grafik Network Simulator* (GSN3) dimana *software* tersebut berguna untuk melakukan uji simulasi dan analisis jaringan yang realistis. Pada penelitian tersebut *parameter* pengujian yang

diuji adalah waktu *round-trip* (RTT) dan waktu konvergensi. Dimana waktu *round-trip* adalah waktu yang diperlukan paket data dari pengirim menuju ke penerima dan akan diterima lagi ke pengirim, untuk mengetahui *round-trip* dapat menggunakan pengiriman paket PING ke alamat tujuan, dalam pengujian ini ada beberapa hal yang dapat mempengaruhi proses pengiriman paket, diantaranya kecepatan data, *transfer rate*, media transmisi yang digunakan, dan jumlah *node* yang dilewati. Kemudian waktu konvergensi adalah waktu yang diperlukan *router* dalam sebuah jaringan untuk mengenali jaringan dan menetapkan rute untuk ke setiap jaringan [9].

Pada penelitian yang berjudul "Analisis Kinerja Redistribusi *Routing* Protokol Dinamik (Studi Kasus : RIP, EIGRP, IS-IS)" yang ditulis oleh Chairul Mukmin dan Edi Surya Negara. Tujuan dari penelitian ini adalah untuk menganalisis perbandingan *routing* redistribusi pada protokol *routing* RIP, EIGRP, dan IS-IS serta mengetahui protokol mana yang lebih baik pada jaringan *redistribusi* menggunakan *parameter throughput, delay,* dan *packet loss*. Penelitian ini menggunakn GNS3 menggunakan *router* seri Cisco7200 dengan 12 PC *Virtual* (VPCS) yang bertindak sebagai *host*, 8 *switch* dengan *port gigabyte*, dan *server* yang menjalankan Windows XP. Paket yang dikirim berupa ICMP dengan ukuran 6000 byte dan waktu 5 menit pada setiap skenario [10].

Pada penelitian yang berjudul " *An Approach to Performance and Qualitative Analysis of Routing Protocols on IPv6*" yang ditulis oleh Md. Maruful Hasan Sabbir, Md. Toukidul Islam, dkk. Dimana penelitian ini bertujuan untuk melakukan pengujian IPv6 dalam *streaming* audio dan video. Penelitian tersebut menggunakan tiga protokol *routing* yang berbeda yaitu RIPng, OSPFv3, dan EIGRP dengan menggunakan simulator OPNET, *parameter* pengujian dalam penelitian tersebut menggunakan QoS seperti *dellay, Jitter*, dan nilai MOS yang digunakan untuk mengevaluasi kinerja IPv6. Dari hasil penelitian tersebut menunjukan bahwa protokol *routing* RIPng memiliki kinerja yang lebih baik dalam lalu lintas yang dikirim dan diterima untuk layanan video. Sedangkan untuk layanan suara menunjukan

protokol *routing* EIGRP memiliki kinerja yang baik dalam lalu lintas data yang dikirim dan diterima [11].

Pada penelitian yang berjudul " *Analysis and Comparative Study for Developing Computer Network in Terms of Routing Protocols Having IPv6 Network Using Cisco Packet Tracer*" yang ditulis oleh Moshammad Sharmin dan Mohammad Anawar Hossain. Penelitian ini bertujuan untuk menemukan kinerja dan keunggulan dalam jaringan IPv6 berdasarkan protokol *routing* RIPng, OSPFv3, EIGRPv6. Pengujian dalam penelitian tersebut menggunakan *cisco packet tracer* dengan menggunakan topologi ring dengan masing-masing menggunakan 3 buah *router*, 5 *switch*, dan 9 PC untuk setiap topologi dan protokol *routing*. Pengujian dilakukan dengan menggunakan perintah ping, kemudian data simulasi akan dikumpulkan dan digunakan untuk membuat perbandingan kinerja protokol [12].

Penelitian lain yang berjudul "Studi komparasi Kinerja dari Adaptive *Routing* Protokol OSPFv3, RIPng, EIGRP IPv6, dan IS-IS pada Jaringan IPv6" yang ditulis oleh Reynaldi Firman Trisanto, dkk. Tujuan penelitian yaitu untuk membandingkan protokol *routing* OSPFv3, RIPng, EIGRP IPv6, dan IS-SI pada jaringan IPv6. Dimana pada penelitian tersebut menggunakan GNS3 sebagai simulator pengujian dengan menggunakan *router* cisco C7200ISO yang mempunyai empat *interface*. Dalam pengujian topologi yang digunakan yaitu topologi *Full Mesh* dengan empat *router*, topologi *Partial Mesh* dengan enam *router*, dan topologi *Partial Mesh* dengan delapan *router*. Dari hasil topologi yang telah dibuat dilakukan pengujian, pengujian pertama yaitu *packet loss* dan *convergence time* untuk mengetahui menggunakan pengiriman paket ICMP dari *router* pengirim ke *router* penerima. Kemudian pengujian kedua yaitu pengujian RTT untuk mendapatkan nilai terkecil dari rata-rata RTT. Nilai terkecil dalam rata-rata RTT digunakan sebagai rujukan dalam menentukan kinerja *routing* terbaik. Pengujian RTT dilakukan dengan cara mengirim paket ICMP dari *router* pengirim ke *router* tujuan dengan besaran paket sebesar 250 byte dan *time out* sebesar 2 detik dan dilakukan sebanyak 75 kali [5] .

Pada penelitian yang berjudul *" Performance Evaluation of IPv6 Network for Real-Time Applications using IS-ISv6 Routing Protocol on Riverbed Modeler*" yang ditulis oleh Nehan Jain dan Ashis Payl. Penelitan tersebut dilakukan untuk melakukan evaluasi kinerja jaringan IPv6 dengan menggunakan *routing* protokol IS-ISv6 untuk aplikasi yang membutuhkan pertukaran data *real-time* yang disimulasikan pada *riverbed modeler* akademik edisi 17,5. Tujuan dari penelitian ini untuk mengetahui kinerja *routing* protokol IS-ISv6 dalam merutekan lalu lintas. Pengujian pada penelitian tersebut menggunakan paket data video dan suara, hasil dari *throughput* pada pengujian tersebut menunjukan bahwa paket data berupa video memiliki persentase 84,3% dan paket data suara memiliki persentase 56,5%. Sedangkan untuk *delay* paket data suara lebih tinggi dibandingkan paket data video yaitu 9,7 paket/detik untuk suara dan 24 milidetik untuk video [13].

Pada penelitian yang berjudul "*Performance Analysis of Dynamic Routing Protocols in IPv6 and IPv4 Networks*" yang ditulis oleh Neha Jain, Ashish Payl, Aarti Jain. Penelitian ini ditulis untuk melakukan perbandingan antara protokol *routing* RIP untuk jaringan IPv4 dan RIPng untuk jaringan IPv6 dengan pengujian menggunakan beberapa *parameter* yang berbeda seperti *File transfer protocol* (FTP), DB Query (database), dan surat elektronik *(email)* selain itu juga menggunakan pengujian QoS seperti *throughput, delay, jitter*. Simulasi pengujian pada penelitian ini menggunakan *Riverbed Modeler* atau OPNET dengan menggunakan *router* Cisco sebagai alat pengujian [14].

Tabel 2. 1 Tabel Penelitian Sebelumnya

No	Judul	Penulis	Perbedaan	Hasil
1.	*QoS Analysis on OSPFv3 and RIPng Using GRE Tunneling on IPv6 Integrated IPv4 Network* [8]	Indra Warman, Alex Franzoal(2018)	Dalam penelitian ini menggunakan enam buah *router* yang dibagi menjadi dua area, dan terdapat komputer *client* dan *server* yang terhubung dengan menggunakan IPv6 dimana menggunakan *routing* protokol RIPng dan OSPFv3. Sedangkan untuk penelitian penulis menggunakan FRR (*Free range router*) dan menggunakan protokol *routing* RIPng dan IS-IS.	Hasil dari penelitian ini adalah mencari QoS dengan menggunakan protokol *routing* OSPFv3 dan RIPng menggunakan *tunnel* GRE. Didapatkan hasil bahwa protokol *routing* OSPFv3 menggungguli RIPng dalam *parameter* d*elay, packet loss* dan *throughput*. Penggunaan protokol *routing* mempengaruhi hasil yang diperoleh.
2.	Analisis Perbandingan Kinerja Protokol *Routing* OSPF, RIP, EIGRP, dan IS-IS [9]	Pahlevi Muhammad, Primantara Hari Triswan,	Pengujian penelitian ini menggunakan beberapa jenis *router* cisco dan menggunakan beberapa jenis topologi yang berbeda	Hasil penelitian ini menunjukkan bahwa protokol EIGRP memiliki manfaat untuk pengujian *round trip time* baik pada IPv4 maupun IPv6.

No	Judul	Penulis	Perbedaan	Hasil
		Kasyful Amron (2019)	sedangkan pengujian penelitian penulis menggunakan *router* FRR	Kedua protokol *routing* IS-IS memiliki nilai rata-rata terendah ketika diuji pada jaringan IPv6. Selain itu, RIPngi memiliki nilai terendah yang di uji pada topologi 4 *router* dan 5 *router*, sedangkan OSPFv3 berkinerja lebih baik pada topologi 8 *router*
3.	Analisi Kinerja Redistribusi *Routing* Protokol Dinamik (Studi Kasus : RIP, EIGRP, IS-SI) [10]	Chairul Mukmin, Edi Surya Negara (2019)	Dalam penelitian ini menggunakan *router* Cisco 7200 Series serta menggunakan IPv4 sebagai alamat IP. Sedangkan untuk penelitian penulis menggunakan FRR dan menggunakan alamat IPv6 sebagai alamat IP.	Hasil dari penelitian ini menunjukan bahwa protokol *routing* RIP redistribusi IS-IS memiliki nilai yang lebih dalam *throughput*. Kemudian nilai RIP redistribusi EIGRP memiliki nilai yang lebih baik dalam d*elay*. Kemudian untuk p*acket loss* semua protokol *routing* memiliki nilai yang sama
4.	*An Approach to Performance and*	Md. Maruful Hasan Sabbir,	Dalam penelitian ini menggunakan layanan *streaming* baik video maupun	Hasil dari penelitian ini adalah untuk melakukan evaluasi kinerja layanan

No	Judul	Penulis	Perbedaan	Hasil
	Qualitative Analysis of Routing Protocols on IPv6 [11]	Md. Toukidul Islam, Syed Zahidur Rashid, Abdul Gafur, Md. Humayun Kabir (2019)	suara dan menggunakan OPNET untuk melakukan simulasi jaringan, sedangkan untuk penelitian penulis menggunakan GNS3 dan QoS dengan *parameter throughput, delay, jitter,* dan *packet loss*	*streaming* video pada jaringan IPv6. Dimana hasilnya menunjukan bahwa *routing* RIPng mempunyai hasil kinerja terbaik dalam lalu lintas data yang dikirim maupun diterima untuk paket data video serta VOIP. Sedangkan EIGRP menunjukan performa terbaik untuk *end to end delay* pada layanan video.
5.	*Analysis and Comparative Study for Developing Computer Network in Terms of Routing Protocols Having IPv6 Network Using Cisco Packet Tracer* [12]	Moshammad Sharmin Akter, Mohammad Anwar Hossain (2019)	Dalam penelitian ini menggunakan Cisco paket tracer untuk melakukan pengujian, sedangkan untuk penelitian penulis menggunakan GNS3	Hasil dari penelitian ini yaitu untuk menemukan kinerja terbaik dalam IPv6 dengan menggunakan protokol *routing* RIPng, OSPFv3, dan EIGRPv6. Dengan menggunakan simulasi Cisco Paket Tracer. Dimana tujuan penelitian ini untuk menganalisis waktu yang dihasilkan oleh masing-masing *routing* protokol. Hasil menunjukan bahwa

No	Judul	Penulis	Perbedaan	Hasil
				protokol *routing* EIGRPv6 relatif lebih baik dibandingkan dengan RIPng dan OSPFv3. *Routing* protokol RIPng lebih unggul jika menggunakan jaringan dengan skala kecil dan OSPFv3 memiliki keunggulan dalam jaringan dengan skala besar. EIGRPv6 memberikan waktu konvergensi yang lebih cepat, meningkatkan skalabilitas, dan penanganan dalam perutean.
6.	Studi komparasi Kinerja dari Adaptive *Routing* Protokol OSPFv3, RIPng, EIGRP IPv6, dan IS-IS pada Jaringan IPv6 [5]	Reynaldi Forman Tersianto, Nurul Hidayat, Heru Nurwasito (2020)	Dalam penelitian ini menggunakan *router* Cisco C7200 IOS dengan menggunakan *interface fastEthernet* untuk menghubungkan antar *router*. Sedangkan untuk penelitian penulis menggunakan FRR sebagai *router* yang digunakan untuk melakukan konfigurasi *routing* dengan IPv6.	Hasil dari penelitian ini didapatkan bahwa protokol *routing* OSPFv3 dan IS-IS memiliki *convergence time* yang lebih unggul dalam skenario topologi empat *router*, enam *router*, dan delapan *router*. Kemudian berdasarkan nilai rata rata RTT protokol *routing* IS-IS memiliki kinerja yang lebih baik

No	Judul	Penulis	Perbedaan	Hasil
				karena IS-IS dapat mentransmisikan *ICMP echo Message* ke *node* tujuan dengan cepat dan penerima merespon *node* dengan mentransmisikan ICMP *echo reply* secara cepat.
7.	*Performance Evaluation of IPv6 Network for Real-Time Applications using IS-ISv6 Routing Protocol on Riverbed Modeler* [13]	Siti Ummi Masruroh, fadly Robby, Nashrul Hakiem (2020)	Dalam penelitian ini menggunakan *router* cisco 3725 series untuk *router* dengan topologi menggunakan tujuh unit *router* dengan menggunakan koneksi serial DTE/DCE dan dua koneksi tembaga. Sedangkan penelitian penulis menggunakan *router* FRR (*Free Range Routing*) dengan menggunakan topologi *mesh full connection*.	Hasil dari penelitian ini adalah nilai *throughput* untuk video 84,3% dan suara 56,5%. Dimana untuk paket data suara memiliki nilai yang rendah karena turunnya trafik IPv6. Namun untuk paket suara memiliki nilai yang lebih baik untuk *parameter* d*elay*. Kemudian untuk *parameter Jitter* didapatkan nilai sebesar 184 *milisecond* untuk paket data suara.
8.	*Performance Analysis of Routing Protocols On IPv4*	Neha Jain, Ashish Payl,	Dalam penelitian ini menggunakan *router* cisco sebagai *router* pengujian dan menggunakan protokol *routing*	Hasil dari penelitian ini yaitu menunjukkan perbandingan kinerja protokol *routing* RIP pada jaringan

No	Judul	Penulis	Perbedaan	Hasil
	and IPv6 Addressing Networks [14]	Aarti Jain (2021)	RIP untuk jaringan IPv4, dan menggunakan protokol *routing* RIPng untuk jaringan IPv6. Sedangkan untuk penelitian penulis menggunakan FRR sebagai *router* dengan membandingkan protokol *routing* RIPng dan IS-IS dengan menggunakan GNS3 sebagai simulasi jaringan.	IPv4, dan kinerja protokol *routing* RIPng pada jaringan IPv6. Pengujian simulasi tersebut digunakan untuk aplikasi *real-time* dimana hasilnya akan digunakan untuk analisis. Protokol *routing* RIPng pada jaringan IPv6 memiliki efisiensi trafik yang lebih baik dibandingkan RIP pada jaringan IPv4. Hal ini disebabkan karena RIPng pada jaringan IPv6 karena penundaan ethernet yang lebih rendah dan konvergensi yang lebih pendek. Keduanya memiliki kelebihan masing-masing namun harus disesuaikan dengan kebutuhan kinerjanya.

penelitian sebelumnya, dapat ditarik kesimpulan bahwa pengujian penelitian sebelumnya melakukan pengujian dengan berbagai kombinasi protokol *routing*, topologi dan pengujian yang dilakukan akan mempengaruhi hasil dari pengujian. Selain itu penelitian sebelumnya juga melakukan evaluasi kinerja protokol *routing* seperti OSPFv3, RIPng, EIGRP, dan IS-IS dalam jaringan IPv6. Dimana setiap penelitian terdahulu menunjukkan perbedaan dalam kinerja protokol *routing* dalam menangani lalu lintas data *real-time* maupun *non-real-time*. Dari beberapa penelitian tersebut juga memberikan hasil rekomendasi pemiliihan protokol *routing* untuk kondisi tertentu serta pengaruh faktor-faktor seperti *konvergensi*, efisiensi waktu dan *respone time.* Dimana dari penelitian sebelumnya akna memberikan gambaraan tentang protokol *routing* dalam beberapa kondisi tertentu. Kolom hasil penelitian memberikan gambaran hasil dari penelitian yang telah dilakukan sebelumnya. Sehingga dapat memberikan pengetahuan atau referensi untuk penelitian yang akan datang

2.2. Dasar Teori

2.2. 1. Internet Potocol Version 6

IPv6 merupakan sebuah protokol pengalamatan yang dikembangkan oleh IETF. Pengembangan protokol ini dilakukan karena kebutuhan alamat IPv4 yang tidak bisa menampung alamat IP yang banyak. Kelebihan IPv6 yaitu panjang alamat yang luas, dengan panjang 128-bit dimana terdiri dari 8 blok, dan di setiap blok terdiri dari 16 bit. Dengan demikian alamat IPv6 memiliki jumlah alamat yang sangat banyak, yaitu sekitar 3,4 x 10^38 atau setara dengan 340 *undecillion* alamat IP atau angka 0 dengan jumlah sebnayak 36 *digit* [1]. Dimana hal ini akan memberikan keuntungan untuk pertumbuhan kebutuhan alamat IP di masa depan.

IPv6 mempunyai kelebihan dibandingkan dengan IPv4 selain dari jumlah IP yang tersedia lebih banyak, salah satunya adalah mengatasi masalah yang diakibatkan oleh *Network Address Translation* (NAT). Dalam IPv4 NAT dapat menghambat dalam komunikasi dua arah secara real-time. Dalam IPv6 NAT tidak digunakan sehingga komunikasi dapat berjalan

dengan baik. IPv6 juga mempunyai kemampuan dalam mendukung QoS yang lebih baik. Dalam IPv6 QoS memungkinkan untuk pengguna untuk memprioritaskan paket tertentu seperti prioritas *bandwidth* [15]. Selain itu juga IPv6 mempunyai kelebihan di bagian keamanan yang lebih baik dibandingkan dengan IPv4. Dalam lalu lintas IPv6 dapat dilakukan pengamanan seperti otentikasi, integritas data, dan kerahasiaan data. Hal ini memungkinkan untuk komunikasi data yang lebih baik dan aman [1].

Penulisan alamat IPv6 menggunakan notasi *hexadecimal* dimana pemisah untuk setiap oktet menggunakan titik dua contoh nya : 2001:0db8:0000:0000:0056:abcd:0000:1234, dalam satu oktet terdiri dari 16-bit. IPv6 juga memiliki beberapa aturan yang dapat digunakan, contohnya pada alamat IPv6 diatas dapat disederhanakan dengan cara sebagai berikut :

1. Jika terdapat deret angka (0) dapat disederhanakan menjadi dua tanda titik ”::”, sebagai contoh 2001:0db8:0000:0000:0056:abcd:0000:1234 alamat tersebut dapat disederhanakan menjadi 2001:0db8::0056:abcd:0000:1234. Namun penggunaannya hanya bisa digunakan sekali dalam satu alamat IPv6.
2. Angka 0000 dapat disingkat menjadi 0, sebagai contoh : 2001:0db8::0056:abcd:0000:1234 dapat singkat menjadi 2001:0db8::0056:abcd:0:1234
3. Angka 0 pada awal hextet dapat dihilangkan sebagai contoh : 2001:0db8::0056:abcd:0:1234 dapat disederhanakan menjadi 2001:db8::56:abcd:0:1234

IPv6 mempunyai beberapa jenis alamat yang dapat digunakan antaranya :

1. *Unicast address*

   Unicast address IPv6 dapat digunakan jika ingin mengirimkan data dari satu tujuan ke perangkat tujuan tertentu [1]. Unicast *address* terdapat beberapa jenis diantaranya :

   a. *Global unicast address*

      Global unicast address merupakan alamat IPv6 yang dapat digunakan secara global di seluruh internet. Alamat ini merupakan jenis alamat IPv6 yang paling banyak digunakan. Karakteristik dari *global unicast address* sebagai berikut :

      - Tidak ada alamat yang sama dalam jaringan IPv6 global.
      - Alamat ini digunakan untuk identifikasi perangkat yang terhubung langsung ke internet
      - Alamat ini ditetapkan oleh SLAAC (*Stateless Address Autoconfiguration*)
      - Alamat ini digunakan untuk komunikasi secara global di seluruh internet.
      - Penulisan *Global unicast address* seperti berikut : ”2000::/3”

   b. *Link-local address*

      Link-local address merupakan sebuah alamat yang berlaku dalam satu segmen jaringan lokal (LAN). Karakteristik dari *Link-local address* sebagai berikut :

      - Hanya berlaku dalam jaringan local. Alamat ini tidak dapat berkomunikasi secara langsung ke internet atau internet publik. Tujuan dari alamat ini yaitu untuk

berkomunikasi antar perangkat dalam satu jaringan lokal.

- Alamat ini digunakan untuk identifikasi perangkat dalam jaringan lokal. Hal ini memungkinakn setiap perangkat didalam jaringan lokal dapat saling terhubung dan bertukar informasi.
- Penulisan notasi *Link-local address* seperti berikut ini : “fe80::/10”

c. *Unique local address* (ULA)

Unique local address merupakan alamat IPv6 yang dirancang untuk jaringan lokal yang dirancang untuk jaringan pribadi dan lokal[1]. Karakteristik dari *Unique local address* sebagai berikut :

- Alamat *unique local address* tidak dapat dirutekan di internet publik, alamat ini dirancang dan digunakan dalam jaringan lokal dan tidak bisa digunakan untuk komunikasi ke internet dan tidak akan terjadi konflik dengan alamat IPv6 global.
- Dalam setiap perangkat memiliki alamat yang unik dan berbeda.
- Penulisan alamat *unique local address* seperti berikut : “fc00::/7” alamat tersebut menunjukan bahwa alamat tersebut masuk kedalam *unique local address*.

2. *Multicast address*

Alamat *multicast address* merupakan jenis alamat dalam protokol jaringan yang digunakan untuk mengirimkan data dari satu pengirim atau beberapa pengirim ke banyak

penerima dalam satu waktu. Hal ini akan memberikan efisiensi waktu dalam distribusi data ke beberapa tujuan tanpa harus mengirimkan salinan data ke setiap penerima secara terpisah [1].

Penulisan alamat *multicast address* terdiri dari delapan blok *heksadecimal,* dimana untuk awalan menggunakan ”ff’ hal ini menunjukan bahwa alamat tersebut adalah alamat *multicast*. Contoh penulisan *multicast address* sebagai berikut : ”ff01::1”. Penggunaan *multicast address* digunakan dalam protokol yang mendukung layanan media streaming seperti video konferensi atau IPTV yang penggunaannya harus dikirimkan ke banyak perangkat secara bersamaan.

3. *Anycast address*

Anycast address adalah salah satu jenis alamat dalam protokol jaringan IPv6 yang digunakan untuk mengarahkan lalu lintas jaringan ke salah satu atau beberapa perangkat yang memiliki alamat yang sama, lalu lintas jaringan akan diarahkan ke satu perangkat terdekat atau memiliki lintasan terpendek dalam jaringan. Dalam *anycast address* setiap perangkat dapat menggunakan alamat yang sama [1].

Anycast address digunakan untuk mencapai tujuan redundansi dan ketersediaan yang tinggi dalam sebuah jaringan. Dengan mengalokasikan beberapa perangkat dengan alamat *anycast* yang sama pada perangkat yang berbeda, dimana jika satu perangkat mengalami masalah maka lalu lintas akan diarahkan ke perangkat yang lain yang masih berfungsi. Pemilihan *node* biasanya didasarkan pada kriteria seperti jarak terpendek atau ketersediaan sumber daya yang optimal.

2.2. 2. Routing Protokol

Routing protokol adalah cara untuk menemukan jalur terbaik untuk mengirim paket data dari pengirim ke penerima. Selain itu *routing* adalah proses yang memungkinkan perangkat di jaringan berbeda untuk berkomunikasi satu sama lain. Pengiriman paket data pada *routing* menggunakan IP *address* untuk saling terhubung [16][17] . Dalam pertukaran data *router* akan bertukar informasi *routing* tabel yang menampilkan informasi *routing* pada perangkat lain. Beberapa protokol *routing* yang mendukung IPv6 yaitu RIPng, EIGRP, OSPFv3, IS-IS dan BGP IPv6.

2.2. 3. Routing Information Protocol next generation (RIPng)

Routing Information Protocol next generation atau RIPng adalah versi protokol *routing* RIP (*Routing Information Protocol*) yang dikembangkan untuk mendukung jaringan IPv6, dimana IPv6 memiliki panjang alamat yang lebih panjang dibandingkan dengan IPv4. RIPng merupakan protokol *routing* yang berbasis *distance-vektor* dimana RIPng akan bertukar informasi *routing* dalam bentuk vektor jarak atau jumlah loncatan dari *router* ke tujuan yang dituju [9].

2.2. 4. Intermediate System to Intermediate System (IS-IS)

Intermediate System to Intermediate Syste atau IS-IS adalah protokol *routing* yang digunakan dalam jaringan komputer dengan cakupan yang luas dan kompleks seperti jaringan telekomunikasi dan ISP (*Internet Service Provider*). IS-IS merupakan protokol *routing* yang berjalan pada Layer 3 OSI (*Open Systems Interconnection*) yang digunakan untuk mengelola perangkat atau *node* jaringan.

IS-IS mengatur lalu lintas data yang dikirim antar berbagai domain yang terhubung. Protokol IS-IS berbasis *Link-state* dimana setiap perangkat dalam jaringan memiliki pemahaman yang lengkap tentang topologi jaringan dan akan disimpan dalam bentuk database yang disebut LSDB

(*Link-state Database*). Informasi tersebut akan digunakan untuk menghitung jalur terbaik dalam mengirim lalu lintas data [6]. IS-IS juga mendukung konsep hirarki yang memungkinakn jaringan besar untuk dipecah menjadi area yang lebih kecil yang berfungsi untuk mengelola skalabilitas. Dimana setiap area mempunyai satu atau lebih *router* yang disebut L1 dan satu atau lebih *router* yang disebut L2. L1 memiliki tanggung jawab untuk pertukaran informasi dalam area itu, sedangkan L2 memiliki tanggung jawab untuk pertukaran informasi antara area.

2.2. 5. Free Range Routing (FRR)

Free Range Routing adalah *routing* open source yang dikembangkan oleh *Quangga* dan *Zebra* pada tahun 2017. *Free Range Routing* merupakan perangkat lunak *open-source* sehingga dapat digunakan secara gratis dan dapat dikembangkan sendiri hal tersebut memberikan keuntungan kepada pengguna tanpa harus bergantung pada perangkat keras dan perangkat lunak yang berbayar. *Free Range Routing* menyediakan layanan perutean standar seperti BGP (*Border Gateway Protocol*), RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*), IS-IS (*Intermediate System to Intermediate System*) [18].

Free Range Routing dapat diinstall di berbagai jenis sistem operasi seperti Distro Linux, FreeBSD, OpenBSD, dan macOS, maka dari itu FRR lebih mudah digunakan dan lebih fleksibel. Selain itu, *Free Range Routing* merupakan bagian dari *Linux Foundation* dimana FRR mempunyai jalur potensial dalam pengujian yang lebih luas dan penerapan modifikasi.

2.2. 6. Graphical Network Simulator-3 (GNS3)

GNS3 (*Graphical Network Simulator 3*) merupakan sebuah *software* simulasi jaringan berbasis *open source* yang bisa melakukan emulasi jaringan yang kompleks. GNS3 menggunakan tiga prinsip yaitu simulasi, emulasi dan *Virtual*isasi. Keunggulan dari GNS3 dapat diintegrasikan ke jaringan fisik yang sudah ada. Dimana GNS3 dapat merealisasikan *interface*, *router*, dan perangkat jaringan yang ada. GNS3 juga dapat

didukung dengan *software* emulator lainya seperti VMware, *Virtual*box. *Software* ini dapat digunakan untuk berbagai jenis sistem operasi sehingga penggunaanya lebih mudah [19].

Software GNS3 juga memiliki beberapa kelebihan dibandingkan dengan aplikasi emulasi lainnya. Dimana hal ini akan memberikan keuntungan dalam pengembangan dan simulasi jaringan yang lebih baik. Berikut ini beberapa kelebihan dari GNS3:

1. Dapat digunakan untuk membuat jaringan dengan topologi yang kompleks, dimana GNS3 dapat digunakan untuk menggunakan berbagai jenis perangkat jaringan *Virtual* untuk membangun serta merancang jaringan yang kompleks, sehingga dapat mensimulasikan jaringan yang realistis.
2. Kompatibel dengan berbagai jenis perangkat jaringan. GNS3 dapat melakukan simulasi berbagai jenis komponen jaringan yang ada dan bisa dikombinasikan seperti dapat menggunakan perangkat Cisco, Mikrotik, Linux, Windows *Server*, dan berbagai jenis firewall yang ada.
3. Dapat melakukan koneksi dengan jaringan fisik: Dimana hal ini dapat digunakan untuk menghubungkan topologi jaringan yang ada dalam GNS3 ke jaringan fisik yang nyata.
4. Intergasi dengan software Wireshark. GNS3 dapat digabungkan dengan wireshark hal ini memungkinkan pengguna dapat menganalisis jaringan yang telah dibuat. Wireshark sendiri merupakan sebuah software yang digunakan untuk melakukan analisis lalu lintas jaringan (*tools packet capture analyzer*).

2.2. 7. Quality of Service (QoS)

Quality of service (QoS) merupakan sebuah teknik dalam mengelola kapasitas dalam jaringan. QoS lebih mengacu pada kemampuan dalam menyediakan layanan yang lebih baik dalam pengiriman berbagai jenis data.

Qos juga dapat digunakan untuk memberikan prioritas lalu lintas data tertentu. *Parameter* QoS yang digunakan seperti *Throughput, Delay, Jitter, Packet loss* [20].

1. *Throughput*

Throughput adalah kecepatan transfer data yang aktual pada jaringan. *throughput* sering kali disebut dengan *bandwidth. throughput* bersifat dinamis karena bergantung pada lalu lintas data yang terjadi [21]. Kecepatan pengiriman data dalam jaringan dipengaruhi oleh beberapa faktor seperti jenis *port* yang digunakan dan lalu lintas yang ada dalam jaringan. Dalam *throughput* semakin besar nilainya maka semakin bagus pula kemampuan jaringan dalam mengirimkan data. Jika dalam suatu jaringan terdapat lalu lintas yang tinggi maka nilai *hroughput* akan mengalami penurunan karena terjadi penghambatan dalam pengiriman data. Untuk mendapatkan nilai *throughput* dapat menggunakan persamaan 2.1 berikut :

$$Throughput = \frac{Jumlah\ data\ yang\ diterima}{Waktu\ pengiriman\ data} \quad (2.1)$$

2. *Delay*

Delay atau *latency* adalah waktu yang dibutuhkan oleh suatu paket data untuk sampai dari pengirim menuju penerima. Ada beberapa faktor yang menyebabkan *delay* diantaranya media transmisi yang digunakan, kemudian ukuran paket data juga salah satu faktor dimana semakin besarnya paket data yang dikirim maka membutuhkan sedikit lama waktu yang diperlukan agar paket data sampai ke tujuan [21]. Untuk mendapatkan nilai *delay* dapat menggunakan persamaan 2.2 berikut :

$$Delay = Waktu\ penerimaan\ paket - waktu\ pengiriman\ paket \quad (2.2)$$

3. *Jitter*

Jitter atau penundaan dalam suatu jaringan dapat diartikan sebagai variasi kedatangan paket yang disebabkan oleh variasi anjang antrian, waktu pengelolaan data, bahkan waktu perakitan kembali paket dikahir proses *Jitter*. Hal ini dikarenakan beberapa paket akan mengalami penundaan yang lebih besar dibandingkan dengan yang lainnya [22]. Dalam jaringan *Jitter* mempunyai dampak negatif, terutama gangguan dalam aplikasi *real-time* dimana dapat menyebabkan gangguan dalam aplikasi yang memerlukan waktu respon yang konsisten dan cepat, seperti komunikasi *real-time* dan layanan video *streaming*. Dimana variasi *delay* yang tinggi dapat menyebabkan gangguan dalam aliran data dan performa yang buruk dalam aplikasi. Untuk mendapatkan nilai *jitter* dapat menggunakan persamaan 2.3 berikut :

$$Jitter = \frac{Total\ variasi\ delay}{Total\ paket\ yang\ diterima} \tag{2.3}$$

4. *Packet loss*

Packet loss merupakan sebuah *parameter* yang mengindikasikan jumlah paket yang gagal mencapai tujuan pada saat proses pengiriman data. Paket data yang hilang bisa disebabkan karena beberapa hal seperti *collision* (tabrakan), *congestion* (kepadatan) trafik jaringan [22]. Dalam perangkat jaringan dilengkapi dengan buffer yang berfungsi menampung data yang diterima, jika terjadi kepadatan lalu lintas data yang berlangsung dalam waktu yang lama, *buffer* akan terisi dan data baru tidak dapat diterima. Untuk mendapatkan nilai *packet loss* dapat menggunakan persamaan 2.4 berikut :

$$Packet\ Loss = \frac{Paket\ dikirim\ -\ Paket\ diterima}{paket\ dikirim} x100\% \tag{2.4}$$

2.2. 8. User Datagram Protocol (UDP)

UDP (*user datagram protocol*) merupakan salah satu protokol berbasis IP. Dimana teknik ini digunakan untuk melakukan koneksi dua titik jaringan. Protokol ini termasuk dalam *connectionless* dimana dalam pengiriman data lebih cepat tanpa memperhatikan paket data yang hilang[23]. Paket UDP dikenal dengan datagram dimana dibagi menjadi dua bagian yaitu *header* dan *playload*. Protokol UDP tidak melakukan proses kontrol alur data, kontrol kesalahan atau pengiriman ulang terhadap kesalahan.

Protokol UDP memiliki beberapa karakteristik seperti berikut :

1. UDP termasuk protokol tanpa koneksi, dimana tidak ada pembentukan, pemeliharaan koneksi sebelum atau sesudah pengiriman data. Dimana setiap paket dianggap sebagai entitas yang independen
2. Tidak menjamin pengiriman data. Dimana pada UDP tidak ada mekanisme yang menjamin bahwa setiap paket yang dikirimkan akan sampai di tujuan dalam urutan yang sesuai.
3. UDP mempunyai *header* yang ringan. Dimana *header* pada UDP terdiri dari beberapa *field*, termasuk *port* pengiriman, *port* tujuan, panjang datagram, dan *checksum*.
4. Setiap paket yang dikirimkan UDP disebut datagram. Dimana setiap datagram merupakan unit yang independen dan tidak bergantung pada datagram sebelumnya maupun sesudahnya. Hal ini memungkinkan pengiriman secara paralel tanpa batasan antara datagram.
5. Digunakan untuk paket data *real-time*. Karena memiliki sifat yang ringan paket UDP cocok digunakan untuk

aplikasi seperti VOIP (*voice over IP*), video *streaming*, dan game *online*.

2.2. 9. Transmision Control Protocol (TCP)

TCP (*transmission control protocol*) merupakan salah satu protokol yang berjalan pada lapisan trans*port* layer dalam model OSI layer (*Open System Interconnection*). TCP digunakan untuk komunikasi yang handal[23].

Protokol TCP mempunyai beberapa karakteristik seperti berikut:

1. Protokol berbasis *Connection-oriented*. Dimana pembentukan koneksi harus dilakukan sebelum pertukaran data, setelah koneksi terbentuk akan ada jalur komunikasi dua arah antara pengirim dan penerima.
2. Proses pembentukan koneksi TCP melibatkan handsake 3 langkah (*three-way-handshake*), yang melibatkan pesan SYN, SYN-ACK, dan ACK dalam pembentukan koneksi.
3. Protokol yang menjamin pengiriman paket. Dimana mekanisme pengiriman ulang dan *acknowledgment* digunakan untuk memastikan bahwa setiap paket yang dikirim akan tiba tanpa kehilangan.
4. TCP menyediakan mekanisme *flow control* yang digunakan untuk mengatur kecepatan pengiriman data agar sesuai dengan penerima.
5. Koneksi TCP mendukung komunikasi *full duplex* dimana pengirim dan penerima dapat melakukan pertukaran data secara bersamaan.

2.2. 10. Wireshark

Wireshark adalah sebuah *tools packet capture analyzer* yang digunakan untuk melakukan analisis paket data dalam sebuah jaringan. Wireshark dapat melakukan pemantauan lalu lintas jaringan baik jaringan

kabel maupun *nirkabel*. Wireshark juga mampu melakukan perekaman paket data yang lewat dimana hal ini bertujuan untuk memecahkan masalah atau memeriksa lalu lintas yang sedang terjadi [19]. Menggunakan wireshark juga bisa melakukan *filtering* paket data yang lewat berdasarkan kriteria seperti alamat IP, *port*, protokol. Wireshark juga bisa digunakan diberbagai jenis sistem operasi seperti windows, macOS, dan linux.

2.2. 1. iPerf3

Iperf3 adalah sebuah *tools* yang digunakan untuk melakukan pengukuran kinerja jaringan. *Parameter* pengukuran yang dapat dilakukan dengan menggunakan iperf3 adalah *throughput, dellay, jitter* [24]. *Tools* iperf3 dikembangkan oleh *Esnet / Lawrance Barkely National Laboratory*. Dirilis di bawah lisensi *three-clause BSD license.*