BAB II TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya/Tinjauan Pustaka

Dalam penelitian ini, peneliti melakukan studi literarur terhadap lima jurnal yang berkaitan dengan topik penelitian. Adapun ringkasan dari jurnal terkait adalah sebagai berikut :

Penelitian sebelumnya berjudul “Implementasi Routing Dinamis OSPFV3 Pada Internet Protocol Versi 6 (IPv6) Menggunakan Router Mikrotik” oleh Andri Maulana di mana penelitian tersebut bertujuan untuk mengimpelentasikan dan melakukan uji QoS pada jaringan IPv6 yang menerapkan protokol routing OSPFv3 untuk komunikasi pada router board mikrotik haplite. Pada penelitian tersebut dilakukan percobaan dengan menerapkan konsep jaringan secara langsung dengan menerapkan protokol routing OSPFv3 pada perangkat router mikrotik di jaringan IPv6. Dalam penelitian ini, NDLC, atau *Life Cycle of Network Development*, digunakan, yang mencakup berbagai tahap mulai dari analisis hingga manajemen.Pada tahap analisis, evaluasi kebutuhan jaringan IPv6 dan pemetaan kebutuhan pengguna dilakukan. Setelah itu, perencanaan jaringan dilakukan, yang mencakup perancangan topologi, alokasi alamat IPv6, dan konfigurasi perangkat mikrotik.[8].

Penelitian lain yang berjudul “Implementasi Routing Protokol Ospfv3 Pada Ipv6 Dengan Menggunakan Metode QoS” milik Nurillah Nayoan, dkk, yang melakukann penelitian tentang pengimplementasian dan perancangan jaringan dari protokol OSPFv3 pada IPv6 menggunakan cisco dengan menerapkan metode QoS. Parameter yang menjadi acuan untuk *Quality of service* (QoS) yaitu *delay, throughput, packet loss* dan jitter menurut standar THIPON. Dengan tujuan untuk mengetahui seberapa layak dan bagus layanan dari routing protokol OSPFv3 pada jaringan IPv6[9].

Pada penelitian yang berjudul “Kajian Perbandingan Performansi Routing Protocol RIPNG, OSPFV3 dan EIGRPV6 Pada Jaringan IPv6” oleh Pauzi Hasan dan Peby Wahyu Purnawan. Di mana dalam penelitian tersebut penulis membandingkan antara roting protocol RIPNG, OSPFv3 dan EIGRPv6 pada jaringan IPv6 untuk mengetahui perbandingan nilai QoS dari ketiga routing

protokol tersebut. *Grafik Network Simulator* 3 (GNS3) adalah perangkat simulasi jaringan yang memungkinkan simulasi dan analisis jaringan yang lebih realistis; uji coba ini menggunakan metode analisis seperti pemantauan proses pembaruan routing, analisis paket ICMPv6, dan pengujian pengiriman paket menggunakan *Real-time Transport Protocol* (RTP) yang berupa aliran audio dan video Fokus utama uji coba ini adalah untuk memahami dan menganalisis bagaimana proses pembaruan routing berlangsung dalam jaringan yang diuji; proses ini mengirimkan informasi tentang topologi jaringan dan rute yang tersedia antara router. Dengan melacak proses ini, dapat dinilai efisiensi dan efektivitas routing jaringan dan Wireshark yang tujuannya untuk mencari tahu routing protokol manakah yang memiliki performansi terbaik dalam pengujian *Real-time Transport Protocol* dari ketiga routing yang digunakan[10].

Penelitian yang berjudul "*Comparative Analysis of OSPFv3/IS-IS and RIPng/IS-IS Mixed Protocols for Real-Time Applications in IPv6 Communication Networks*" oleh Yaw Adjei Asante dan Richard Essah, di mana dalam makalah penelitian ini, dilakukan perbandingan kinerja dua protokol routing campuran, yaitu OSPFv3/IS-IS dan RIPng/IS-IS, dibuat dalam jaringan IPv6. Performa mereka diukur dan dibandingkan dengan simulasi menggunakan *Riverbed Modeller Academic Edition*. Tujuan dari makalah ini terutama untuk menentukan campuran protokol mana yang lebih cocok untuk route traffic di jaringan IPv6. Motivasi utama dari makalah ini adalah untuk mengetahui apakah perbedaan dalam algoritma routing RIPng dan IS-IS akan mengibangi dan menghasilkan kinerja yang lebih baik daripada kombinasi dua protokol routing dari algoritma routing yang sama (OSPFv3 dan IS-IS). Untuk mencapai tujuan dari makalah ini, simulasi dibagi menjadi dua skenario. Skenario pertama adalah topologi jaringan IPv6 yang dikonfigurasi dengan OSPFv3/IS-IS. Skenario kedua adalah salinan dari skenario pertama tetapi dikonfigurasi dengan RIPng/IS-IS. Kedua skenario disimulasikan dan efek penggunaan setiap skenario untuk merutekan aplikasi yang dipilih secara terpisah diukur dan dicatat. Perbandingan kinerja protokol campuran didasarkan pada parameter kuantitatif berikut: waktu respons kueri basis data, lalu lintas kueri basis data yang diterima, waktu respons unggah/unduh email, waktu respons

unggah/unduh ftp, lalu lintas ftp yang diterima, waktu respons halaman http, waktu respons login jarak jauh dan lalu lintas IPv6[11].

Selanjutnya penelitian dengan judul "Analisis Kinerja Routing Protokol Ripng Dengan OSPFv3 Pada Jaringan IPv6 *Tunneling*" oleh Harni Kusniyati, dkk. Pengujian di jaringan tunneling mencakup analisis seleksi saluran pengiriman data, analisis pembaruan routing, analisa kecepatan waktu konvergensi, analis pengiriman berupa paket data tcp, dan analisis *sniffer* paket data. Metode yang digunakan termasuk studi literatur, pemodelan komputer, dan instalasi jaringan. Tujuan penelitian ini adalah untuk menganalisis kinerja dan pengujian protokol routing RIPng dalam hubungannya dengan OSPFv3 routing protocol, sehingga ketika analisis selesai, akan memungkinkan untuk menetapkan seberapa efektif kedua protokol beroperasi di jaringan tunelling IPv6.[2].

.

2. 1 Penelitian Sebelumnya

No	Jurnal/Paper	Metode	Objek	Kesimpulan	Saran
1.	Implementasi Routing Dinamis OSPFV3 Pada *Internet Protocol* Versi 6 (IPv6) Menggunakan Router Mikrotik.[8]	*Reaserch and Development*	Protokol routing OSPFv3 pada mikrotik	Dalam penelitian tersebut hasil yang diperoleh dalam analisi jaringan QoS protokol Ospfv3 sangat baik, dengan *delay* rata-rata 0,716 ms, jitter 0.002 ms, *packet loss* 0%, dan troughput 1525 k untuk file 60 mbps yang dikirim dari satu komputer ke komputer lain..	
2.	Implementasi Routing Protokol *Ospfv3* Pada Ipv6 Dengan Menggunakan Metode Qos.[9]	*Reaserch and Development*	Protokol routing OSPFv3 pada cisco *packet tracer*	Setelah dilakukan pengujian metode *quality of service* (QoS) berdasarkan tiga parameter *throughput*, *delay* dan *packet loss*, diperoleh nilai rata-rata indeks QoS sebesar 3 yang berarti hasil pengujian diperoleh peningkatan kualitas layanan (QoS) yang baik.)-meskipun Setiap pengujian klien-ke-server menghasilkan indeks *throughput* yang lebih rendah, tetapi semua pengujian QoS secara keseluruhan masuk dalam kategori yang baik. Tingkat keberhasilan akses lalu lintas yang digunakan berkisar dari 75 persen hingga 94 persen.	
3.	Kajian Perbandingan Performansi *Routing protocol Ripng, Ospfv3* dan *Eigrpv6* Pada Jaringan Ipv6.[10]	Kualitatif	Routing Protokol Ripng, OSPFv3 dan Eigrp	Hasil dari analisis dan simulasi menggunakan GNS3 dan *Wireshark* menunjukkan bahwa OSPFv3 lebih baik daripada EIGRPv6 dan RIPng dalam hal *routing update* atau saat *link down*. Kemudian, hasil pengujian dianalisis untuk melihat algoritma mana yang lebih baik untuk paket *real-time transport protocol* (RTP). OSPFv3 ternyata lebih baik daripada EIGRPv6 dan RIPng dalam hal *delay*, *packet loss*, *throughput*, dan *jitter*.	

No	Jurnal/Paper	Metode	Objek	Kesimpulan	Saran
4.	*Comparative Analysis of OSPFv3/IS-IS and RIPng/IS-IS Mixed Protocols for Real-Time Applications in IPv6 Communication Networks.*[11]	*Reaserch and Development*	Protokol routing RIPng/IS-IS dan OSPFv3/IS-IS	Hasil penelitian menunjukkan bahwa RIPng/IS-IS bekerja lebih baik dalam waktu respons pengunduhan/pengunggahan email, waktu respons login jarak jauh, penurunan lalu lintas IPv6, Sedangkan gabungan OSPFv3/IS-IS bekerja lebih baik dalam waktu respons kueri basis data. lalu lintas kueri basis data yang diterima, waktu respons undu, dan waktu respons halaman http.	Untuk penelitian mendatang, penelitian dapat dilakukan untuk menggabungkan protokol routing OSPFv3 dan IS-IS sehingga protokol routing ke depannya dapat dikembangkan, dengan mengevaluasi kode sumber dari semua protokol dan memodifikasi kodenya juga.
5.	Analisis Kinerja Routing Protokol RIPng Dengan OSPFv3 Pada Jaringan Ipv6 Tunneling.[2]	*Reaserch and Development*	Routing protokol RIPng dan OSPFv3	Dikarenakan kecepatan waktu konvergen yang lebih cepat, ospfv3 membutuhkan waktu rata-rata 19 detik, sedangkan ripng 178 detik. Analisa menunjukkan bahwa ospfv3 lebih baik dibandingkan ripng. Pengujian *throughput* jaringan dengan paket tcp berukuran 2, 4, 5, 6 kbyte pada windows size menunjukkan nilai rata-rata 121, 58 mbit/sec untuk ospfv3 dan 117, 44 mbit/sec untuk ripng.	1. Dikarenakan banyaknya keterbatasan dalam penggunaan IPvv4, untuk perancangan jaringan selanjutnya disarankan untuk menggunakan IPv6. 2. Jika rancangan jaringan IPv6 kita buat memiliki lingkup yang sangat luas dan kompleks lebih disarankan untuk menggunakan *routing protocol* OSPFv3.

2.2 Dasar Teori

2.2.1 Routing protocol

Protokol routing digunakan agar perangkat dapat berkomunikasi satu sama lain di jaringan yang berbeda dengan menggunakan protokol routing. Selain itu, router dapat merujuk pada proses di mana router memilih rute mana yang tepat untuk mengirimkan atau mengarahkan paket ke jaringan yang dituju, menggunakan IP *address* tujuan untuk mengirim paket, dan memberi tahu router rute mana yang tepat untuk menerusk. Router dapat berbagi data dan informasi routing dengan menggunakan protokol routing[12]. Router dapat bertukar informasi dalam routing table, yang menampilkan informasi tentang jaringan lain yang saling terhubung. Beberapa protokol routing yang mendukung jaringan IPv6 termasuk RIPng, EIGRP untuk IPv6 (properti Cisco), OSPFv3, IS-IS untuk IPv6, dan BGP IPv6.

2.2.2 OSPFv3

OSPFv3 merupakan versi ketiga dan penerus dari OSPFv2 pada protokol routing OSPF yang termasuk dalam bagian dari *Interior Gateway Protocol (IGP)* yang diperkenalkan oleh *Internet Engineering Task Force (IETF)*. OSPFv3 pada dasarnya merupakan protokol routing yang berfokus di jaringan IPv6. Seperti OSPFv1 dan OSPFv2, OSPFv3 juga termasuk protokol routing yang dirancang berdasarkan *link state* untuk mendistribusikan informasi internal ke *autonomous system*. OSPFv3 saat ini digunakan secara luas sebagai protokol routing interior pada jaringan TCP/IP. Konsep dasarnya adalah untuk mengetahui nilai paling rendah dengan menghitung jalur terbaik dalam jaringan yang merupakan jalur terpendek yang tersedia dari jaringan asal ke jaringan tujuan dan proses penerusan hanya menggunakan *next hop* ke tujuan. Setiap router akan memelihara *database*, dimana *database* ini akan berisi seluruh informasi dari setiap router yang terhubung. *Database* ini dikelola oleh masing-masing router[11].

Pada dasarnya, OSPFv3 memiliki jenis paket yang serupa dengan OSPFv2, namun perbedaannya terletak pada kemampuan OSPFv3 dalam mendukung pengalamatan 128-bit yang lebih luas. Dalam OSPFv2, pengalamatan multicast yang digunakan adalah 224.0.0.5 dan 224.0.0.6, sementara dalam OSPFv3,

pengalamatan multicast IPv6 digunakan, yaitu FF02::5 dan FF02::6, untuk tujuan perutean OSPFv3 yang berkaitan dengan Desain Routers (DR) dan Backup DRs (BDR). Selain itu, OSPFv3 menggunakan alamat link-local untuk melakukan pengiklanan (advertisements), dan bukan menggunakan alamat global[8].

Dalam protokol OSPF, terdapat serangkaian paket yang penting yang disebut Link-State Packets (LSP), yang memiliki peran krusial dalam proses perutean OSPF. Pada OSPFv3, terdapat beberapa jenis paket LSP yang berperan dalam pertukaran informasi dan pemeliharaan jaringan, yaitu:

a. Paket *Hello:* Paket *Hello* berguna untuk memulai serta menjaga keterhubungan informasi antara router OSPF yang satu dengan router OSPF yang lain. Paket *Hello* ini membantu router dalam menemukan tetangga OSPF yang berdekatan dan membangun adjacencies (keterhubungan) dengan mereka.
b. DBD (*Packet Database Description*): Paket DBD digunakan untuk memeriksa dan melakukan sinkronisasi *database* antar router dalam jaringan OSPF. Dalam paket DBD, router mengirimkan informasi tentang *database link-state* mereka kepada tetangga OSPF. Ini memungkinkan router tetangga untuk membandingkan dan memperbarui database mereka dengan yang diterima.
c. LSR (*Link-State Request*): Paket LSR digunakan oleh router OSPF untuk meminta informasi yang mungkin tidak ada dalam *database link-state* lokal mereka dari router OSPF lainnya. Dengan mengirimkan paket LSR, router dapat meminta pembaruan atau informasi spesifik yang dibutuhkan untuk memperbarui *database link-state* mereka.
d. LSU (*Link-State Update*): Paket LSU digunakan untuk menjawab permintaan dari paket LSR. Ketika router menerima paket LSR, jika router memiliki informasi yang diminta, router tersebut akan mengirimkan paket LSU yang berisi informasi yang diminta kepada router yang meminta.
e. LSAck (*Link-State Acknowledgment*): Paket LSAck berfungsi sebagai konfirmasi bahwa paket LSU telah diterima oleh router. Setelah

menerima paket LSU, router yang dituju akan mengirimkan paket LSAck sebagai tanggapan, untuk memberi tahu router pengirim bahwa paket LSU telah diterima dengan sukses.[10].

Dengan adanya jenis-jenis paket LSP ini, OSPFv3 memungkinkan router dalam jaringan OSPF untuk saling bertukar informasi, menjaga sinkronisasi database, dan merespons permintaan informasi dari router lainnya. Melalui pertukaran paket-paket LSP ini, OSPFv3 memastikan pemeliharaan dan efisiensi dalam proses perutean jaringan IPv6.

2.2.3 IPv6

IPv6 adalah sebuah standar pengalamatan yang dikembangkan oleh IETF sebagai respons terhadap kebutuhan yang terus berkembang dalam dunia IP. Tujuan utama dari pengembangan IPv6 adalah untuk mengatasi dan meningkatkan kelemahan yang ada pada IPv4. Salah satu kelebihan utama dari IPv6 adalah struktur pengalamatan yang sangat luas, dengan panjang 128-bit yang terdiri dari 8 blok, di mana setiap blok terdiri dari 16 bit[1]. Dengan demikian, IPv6 memiliki kemampuan untuk mengakomodasi sejumlah besar host yang sangat besar, yaitu sekitar 3,4 x 10^38 atau setara dengan 340 undecillion host. Hal ini memberikan skala yang sangat besar dan cukup untuk memenuhi pertumbuhan kebutuhan IP di masa depan.

Salah satu keunggulan utama IPv6 adalah kemampuannya untuk mengatasi masalah yang diakibatkan oleh *Network Address Translation* (NAT). NAT dalam IPv4 seringkali menghambat atau bahkan mencegah aplikasi yang memerlukan komunikasi dua arah secara real-time. Dengan IPv6, masalah NAT dapat diatasi, sehingga memungkinkan aplikasi untuk berkomunikasi secara langsung antara host yang terlibat. IPv6 juga mendukung pengalamatan node dalam hierarki yang lebih besar, yang menyederhanakan proses alokasi alamat. Hal ini memungkinkan pengelolaan alamat yang lebih efisien dan fleksibel di jaringan yang lebih besar. Selain itu, IPv6 juga memiliki kemampuan untuk mendukung QoS (*Quality of service*) yang lebih baik. QoS memungkinkan pengguna untuk menandai paket data pada jenis lalu lintas tertentu yang memerlukan penanganan khusus, seperti

prioritas atau bandwidth yang dijamin. IPv6 juga menyediakan fitur keamanan yang lebih kuat, termasuk dukungan untuk otentikasi, integritas data, dan kerahasiaan data. Ini memungkinkan pengguna untuk mengamankan komunikasi mereka dengan lebih baik dan melindungi data dari ancaman yang mungkin ada di jaringan.Secara keseluruhan, IPv6 adalah sebuah pengembangan yang signifikan dalam dunia pengalamatan IP, memberikan skala yang lebih besar[7].

2.2.3.1 Pengalamatan IP

Pada protokol IPv6, *address* ditulis menggunakan format heksadesimal dengan pemisah titik dua antara setiap blok 16-bit. Format umum untuk penulisan *address* IPv6 dengan x:x:x:x:x:x:x:x, di mana x merupakan empat digit bilangan heksadesimal. Namun, ada beberapa aturan dan teknik untuk meringkas atau menyederhanakan penulisan alamat IPv6.

Sebagai contoh, misalkan kita memiliki alamat IPv6 berikut: 2023:0000:170E:0000:0000:07D0:643B:120A. Terdapat beberapa penyederhanaan yang dapat dilakukan, seperti::

- Angka nol (0) di awal setiap blok adalah opsional. Misalnya, angka 07D0 dapat disederhanakan menjadi 7D0, dan blok 0000 dapat disederhanakan menjadi 0. Dengan demikian, alamat tersebut dapat ditulis menjadi 2023:0:170E:0:0:7D0:643B:120A.
- Urutan angka nol yang ditulis secara berurutan dapat disederhanakan dengan menggunakan tanda "::" (titik dua ganda). Namun, aturan ini hanya dapat digunakan pada sebuah alamat IPv6. Dalam contoh di atas, blok 0000:0000 dapat digantikan dengan "::". Sehingga, alamat tersebut dapat disederhanakan menjadi 2023:0:170E::7D0:643B:120A. [14]

Dengan menggunakan teknik-teknik penyederhanaan di atas, kita dapat mempersingkat penulisan alamat IPv6 yang panjang menjadi bentuk yang lebih ringkas dan mudah dibaca. Hal ini memungkinkan untuk menghemat ruang dan mengurangi kompleksitas dalam penulisan alamat IPv6 yang panjang dan berulang-ulang

Adapun arsitektur pengalamatan pada IPv6 dibagi tiga, yaitu :

- *Unicast Address*

Alamat *unicast* merujuk pada alamat yang ditujukan untuk antarmuka atau host tertentu. Dalam konsep alamat unicast, terdapat tiga jenis alamat yang dapat dibedakan, yaitu:

1. Alamat Link-Local: Alamat ini digunakan dalam satu link atau jaringan lokal. Alamat link-local hanya relevan dan berlaku di dalam jaringan tempat alamat tersebut digunakan. Alamat ini sering digunakan untuk komunikasi antar perangkat pada jaringan lokal tanpa melibatkan perangkat di luar jaringan tersebut.
2. Alamat Site-Local: Alamat site-local dapat dianggap setara dengan alamat private dalam konsep IPv4. Penggunaan alamat site-local terbatas hanya dalam satu site atau area jaringan tertentu. Alamat ini tidak dapat digunakan untuk mengirimkan paket data ke luar site tersebut. Misalnya, jika terdapat beberapa jaringan lokal dalam satu perusahaan, alamat site-local akan digunakan untuk komunikasi internal di antara jaringan-jaringan tersebut.
3. Alamat Global: Alamat global adalah alamat yang dapat digunakan secara publik di seluruh Internet. Alamat ini diperoleh melalui ISP (Internet Service Provider) dan memungkinkan komunikasi antara perangkat di jaringan lokal dengan perangkat di jaringan lain di seluruh dunia. Alamat global memainkan peran penting dalam menghubungkan perangkat dan host secara global melalui Internet.

Dengan membedakan jenis alamat unicast seperti ini, pengguna dapat mengelompokkan penggunaan alamat unicast sesuai dengan kebutuhan jaringan dan tujuan komunikasi. Masing-masing jenis alamat unicast memiliki ruang penggunaan yang terdefinisi dengan cakupan yang sesuai, baik untuk komunikasi dalam jaringan lokal, di antara site-site terbatas, maupun melintasi jaringan global.

- *Multicast Address*

Alamat *multicast* menunjukkan sejumlah antarmuka atau node dalam jaringan, dan ketika paket dikirimkan ke alamat multicast, paket tersebut diteruskan

ke semua antarmuka yang diidentifikasi oleh alamat multicast. Dengan demikian, alamat multicast dapat digunakan untuk mengirimkan paket secara bersamaan ke sejumlah perangkat.

Alamat multicast mengirimkan pesan ke semua host dalam satu jaringan dengan menggabungkan semua bit host menjadi satu, sedangkan alamat broadcast memungkinkan pesan dikirimkan secara bersamaan ke semua perangkat dalam jaringan.

Dalam IPv6, alamat multicast ditempatkan dengan prefiks format IPv6 pada alamat IP. Setiap alamat multicast memiliki prefiks khusus yang membedakannya dari alamat multicast lainnya.

- *Anycast Address*

Alamat *anycast* menunjukkan sejumlah antarmuka atau node dalam jaringan, dan ketika paket dikirimkan ke alamat multicast, paket tersebut diteruskan ke semua antarmuka yang diidentifikasi oleh alamat multicast. Dengan demikian, alamat multicast dapat digunakan untuk mengirimkan paket secara bersamaan ke sejumlah perangkat. Alamat anycast tidak terkait dengan lokasi fisik yang spesifik, tetapi lebih berhubungan dengan konsep jaringan yang memungkinkan paket dikirim ke salah satu node terdekat.

Dalam penggunaan anycast, beberapa node dalam jaringan dapat diberikan prefiks alamat yang sama. Dalam hal ini, semua alamat tersebut dianggap sebagai alamat anycast. Artinya, ketika paket dikirim ke alamat anycast tersebut, jaringan akan memilih salah satu node yang memiliki alamat anycast tersebut untuk menerima dan memproses paket tersebut. Pemilihan node yang tepat biasanya didasarkan pada kriteria seperti jarak terpendek atau ketersediaan sumber daya yang optimal[15][14].

2.2.4 *Free range routing*

Free range routing (FRR) merupakan cabang dari *Quagga* yang dirilis pada tahun 2017 dan ditujukan sebagai alternatif *open-source* untuk implementasi jaringan *routing protocol*s, seperti *Routing Information Protoco*l (RIP), *Open Shortest Path First* (OSPF), *Border Gateway Protocol* (BGP) dan *Intermediate System to Intermediate System* (IS-IS) yang sama dengan perangkat komersial dari

perusahaan seperti Juniper dan Cisco[16]. FRR juga menyertakan proses manajemen informasi routing, untuk bertindak sebagai perantara antara berbagai protokol routing dan ruoter aktif yang diinstal dengan kernel. FRR didukung untuk sistem operasi Linux, OpenBSD, FreeBSD, NetBSD, serta Solaris dan didistribusikan oleh GNU *General Public License* V2 (GPL2). Selain itu, FRR adalah bagian dari *Linux Foundation* yang menjadikan FRR memiliki jalur potensial untuk pengujian yang lebih luas dan penerapan modifikasi yang diusulkan untuk *routing protocol* sekarang, ataupun *routing protocol* baru[17].

2.2.5 GNS 3

GNS3 perangkat lunak simulasi jaringan berbasis grafis, memiliki kemampuan untuk memuat simulasi topologi jaringan dengan lebih kompleks daripada simulator lainnya. Perangkat lunak ini cocok dengan berbagai sistem operasi yang ada, termasuk Windows, Linux, dan MacOS X.[18].

GNS3 memiliki banyak fitur yang mendukung pengembangan dan simulasi jaringan berkualitas tinggi. Beberapa fiturnya adalah:

1. Desain Jaringan yang Berkualitas Tinggi dan Topologi yang Kompleks: GNS3 memungkinkan pengguna menggunakan berbagai perangkat jaringan virtual untuk merancang dan membangun topologi jaringan yang kompleks, yang memungkinkan mereka mensimulasikan konfigurasi jaringan yang realistis dan kompleks..
2. Simulasi *Switch Ethernet*, ATM, dan *Frame Relay*: Fitur GNS3 memungkinkan pengguna untuk menguji dan memvalidasi konfigurasi jaringan yang melibatkan perangkat-perangkat ini.
3. Koneksi dengan Jaringan Fisik: GNS3 memungkinkan pengguna menghubungkan topologi jaringan virtual mereka dengan jaringan fisik nyata. Ini memungkinkan mereka mengintegrasikan dan menguji konfigurasi jaringan virtual mereka dalam lingkungan yang lebih luas.
4. Integrasi dengan Wireshark: GNS3 dapat diintegrasikan dengan Wireshark, sebuah alat yang dirancang untuk menangkap dan menganalisis paket data dalam jaringan. Dengan integrasi ini, pengguna dapat melakukan analisis lalu lintas jaringan yang mendalam pada topologi jaringan virtual yang

dibangun dengan GNS3.Dapat diintegrasikan dengan *Wireshark (tools packet capture*/*analyzer*) untuk analisa *traffic* jaringan.

2.2.6 Quality of service

Metode *Quality of service* (QoS) mengukur kapasitas jaringan dan mendefinisikan fitur dan sifat suatu layanan. Ini adalah arsitektur end-to-end yang tidak dimiliki oleh jaringan. Keandalan jaringan (QoS) mengacu pada kecepatan dan keandalan pengiriman berbagai jenis data selama transmisi data. Administrator jaringan dapat menggunakan QoS untuk memprioritaskan lalu lintas data tertentu.Paket dapat mengalami banyak masalah selama perjalanan dari sumber ke tujuan; ini termasuk *delay*, *throughput*, jitter, dan *packet loss*.[19].

2.2.6.1 Throughput

Throughput mengacu pada kecepatan rata-rata di mana data diterima oleh suatu node dalam jaringan selama periode pengamatan tertentu. Namun, meskipun *throughput* sering kali dikaitkan dengan bandwidth yang telah ditentukan oleh implementasi *physical layer* seperti *Ethernet*, ada sejumlah faktor yang dapat mempengaruhi *throughput* dan membuatnya berbeda dari bandwidth yang terukur.

Salah satu faktor yang berperan dalam menentukan *throughput* adalah jumlah lalu lintas yang ada dalam jaringan. Semakin tinggi jumlah lalu lintas, semakin banyak data yang harus diproses dan dikirim oleh node, yang pada gilirannya dapat mempengaruhi *throughput* secara keseluruhan. Jika jumlah lalu lintas sangat tinggi, *throughput* mungkin mengalami penurunan karena kemungkinan terjadi kemacetan atau penghambatan pada jaringan. Untuk mendapakan nilai *Throghput* dari suatu jaringan dapat didapatkan dari persamaan 2.1 berikut :

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

Klasisfikasi standarisasi nilai *Throughput* berdasarkan TIPHON diuraikan pada tabel berikut :

Tabel 2. 2 standaraisasi *throughput*

Kategori *Throughput*	*Throughput* (bps)	Indeks
Sangat Bagus	>100	4
Bagus	75	3
Sedang	50	2
Buruk	<25	1

2.2.6.2 Delay

Delay merujuk pada waktu yang dibutuhkan oleh sebuah paket untuk melakukan perjalanan dari pengirim ke penerima. *Delay* ini dipengaruhi oleh beberapa faktor, termasuk media transmisi yang digunakan dan ukuran paket data yang dikirim.

Ukuran paket data juga berdampak pada *delay*. Paket data yang lebih besar memerlukan waktu yang lebih lama untuk ditransmisikan daripada paket data yang lebih kecil. Hal ini disebabkan oleh kebutuhan untuk mengirimkan lebih banyak bit melalui media transmisi. Selain itu, dalam beberapa kasus, paket data yang besar mungkin memerlukan pengambilan lebih banyak slot dalam antrian, yang dapat memperpanjang *delay*. *Delay* pada saat transmisi data bisa didapatkan dari perhitungan menggunakan persamaan 2.2 [19].

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

Klasisfikasi standarisasi nilai *Delay* berdasarkan TIPHON diuraikan pada tabel berikut :

Tabel 2. 3 standarisasi *Delay*

Kategori *Delay*	Nilai *Delay* (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 - <300	3

Kategori *Delay*	Nilai *Delay* (ms)	Indeks
Sedang	300 - <450	2
Buruk	>=450	1

2.2.6.3 Jitter

Jitter, dalam konteks jaringan, didefinisikan sebagai variasi dalam *delay* yang terjadi sebagai akibat dari panjang antrian dalam jaringan. Ketika antrian lebih panjang, paket akan mengalami penundaan yang lebih lama sebelum dikirimkan ke tujuan akhir. Hal ini mengakibatkan variasi dalam waktu yang dibutuhkan oleh paket-paket data untuk mencapai tujuan mereka, karena beberapa paket mungkin mengalami penundaan yang lebih besar dibandingkan dengan yang lainnya.

Jitter dapat memiliki dampak negatif dalam komunikasi jaringan, terutama dalam aplikasi yang memerlukan waktu respons yang konsisten, seperti komunikasi real-time atau layanan streaming. Variasi *delay* yang tinggi dapat menyebabkan gangguan dalam aliran data, ketidaksesuaian antara suara dan gambar, atau performa yang buruk dalam aplikasi interaktif.

Untuk mendapakan nilai *Jitter* dari suatu jaringan dapat didapatkan dari persamaan 2.3 berikut :

$$Jitter = \frac{Total\ variasi\ delay}{Total\ paket\ yang\ diterima} \quad (2.3)$$

Variasi *delay* pada persamaan 2.3 diperoleh dari perhitungan menggunakan persamaan 2.4 berikut :

$$Variasi\ Delay = Delay\ 2 - Delay\ 1 \quad (2.4)$$

Klasisfikasi standarisasi nilai *Jitter* berdasarkan TIPHON diuraikan pada tabel berikut :

Tabel 2. 4 Standarisasi Jitter

Kategori	Nilai *Jitter* (ms)	Indeks
Sangat Bagus	0	4
Bagus	>=75 - <125	3
Sedang	>=125 - <226	2
Buruk	225	1

2.3.6.4 Packet loss

Packet loss, merupakan parameter yang mengindikasikan jumlah paket yang terkirim atau hilang dalam suatu kondisi jaringan. Kehilangan paket dapat terjadi karena berbagai faktor, seperti *collision* (tabrakan) atau congestion (kepadatan) dalam jaringan. Biasanya, perangkat jaringan dilengkapi dengan *buffer* yang berfungsi untuk menampung data yang diterima. Namun, jika terjadi kepadatan lalu lintas yang berlangsung dalam waktu yang lama, buffer akan terisi penuh, dan data baru tidak akan dapat diterima.. Untuk mendapakan *Packet loss* dari suatu jaringan dapat didapatkan dari persamaan 2.5 berikut :

$$Packet\ Loss = \frac{Paket\ dikrim - Paket\ diterima}{Paket\ dikirim} x100\% \qquad (2.5)$$

Klasisfikasi standarisasi nilai *Packet loss* berdasarkan TIPHON diuraikan pada tabel berikut :

Tabel 2. 5 standarisasi *packet loss*

Kategori	*Packet loss*	Indeks
Sangat Bagus	0% - <3%	4
Bagus	3% - <15%	3
Sedang	15% - <25%	2
Buruk	>=25%	1

2.2.7 *Wireshark*

Wireshark adalah sebuah perangkat lunak yang digunakan untuk menganalisis paket data dan memecahkan masalah dalam sebuah jaringan. Dengan menggunakan Wireshark mengamati, merekam, dan menganalisis lalu lintas jaringan secara mendetai dan juga dapat mengambil paket data atau informasi yang berlalu-lalang dalam jaringan tersebut. Data yang telah diambil kemudian dapat dianalisis untuk berbagai keperluan.[20]. *Wireshark* dapat disebut juga sebagai *Network Analyzer* yang diibaratkan sebagai alat untuk mencari tahu apa yang sebenarnya sedang terjadi di dalam kabel jaringan dan nantinya informasi yang diperoleh akan ditampilkan[21].

2.2.8 *Iperf3*

Iperf3 adalah *tools* untuk pengukuran aktif bandwidth maksimum yang dapat dicapai pada jaringan IP. *Tools* ini mendukung penyetelan berbagai parameter yang berkaitan dengan waktu, buffer dan protokol (TCP, UDP, SCTP dengan IPv4 dan IPv6). Untuk setiap pengujian, aplikasi ini melaporkan bandwidth, *packet loss*, dan parameter lainnya. Ini adalah implementasi baru yang tidak memiliki kode yang sama dengan dengan versi sebelumnya. *Iperf* pada awalnya dikembangkan oleh NLANR/DAST. *Iperf3* pada prinsipnya dikembangkan oleh *ESnet / Lawrence Berkeley National Laboratory*. *Iperf3* dirilis di bawah *three-clause BSD license*[22].