BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Pada penelitian yang dilakukan oleh Putra, dkk. [7] tahun 2021 membahas tentang perbandingan kinerja metode *single homing* dan *multihoming* menggunakan protokol BGP dalam lingkungan simulasi Eve-NG. Evaluasi dilakukan dengan memperhitungkan waktu konvergensi *routing*, *packet loss*, *delay*, dan *jitter*. Pengujian QoS menunjukkan bahwa untuk parameter *delay*, jaringan yang menggunakan metode *single homing* memiliki rata-rata *delay* sebesar 501.366 ms, sementara pada jaringan yang menggunakan metode *multihoming* memiliki rata-rata *delay* sebesar 501.128 ms. Hasil pengujian QoS juga menunjukkan bahwa tidak ada *packet loss* yang terjadi karena semua paket berhasil terkirim dan diterima. Namun, saat pengujian waktu konvergensi, jaringan yang menggunakan metode *single homing* tidak dapat menghitung waktu konvergensinya karena ketika jaringan terputus, tidak ada *redundant link* sebagai *backup* untuk menghubungkannya kembali. Sebaliknya, pada jaringan yang menggunakan metode *multihoming*, hasil rata-rata waktu konvergensi yang dihasilkan dari pengujian adalah 158.4 detik.

Penelitian Musril. [10] tahun 2017 meneliti mengenai implementasi *Border Gateway Protocol* (BGP) dalam menghubungkan *Autonomous System* (AS) yang berbeda dalam jaringan komputer. Penelitian ini menjelaskan keunggulan BGP dalam menghubungkan AS dan membahas implementasinya menggunakan *software Packet Tracer*. Tujuan penelitian ini adalah untuk menentukan kemampuan BGP dalam menghubungkan AS yang berbeda dan menyediakan simulasi konfigurasi jaringan. Penelitian ini menggunakan metode analisis, desain, pengembangan, dan pengujian. Topologi jaringan dirancang menggunakan Cisco *Packet Tracer*, dan protokol *routing* BGP dikonfigurasi pada *router*. Berdasarkan hasil penelitian, dapat disimpulkan bahwa pengaturan BGP berhasil dalam menghubungkan AS yang berbeda dan memberikan rute terbaik untuk pengiriman paket data dalam jaringan. Penggunaan *routing protocol* BGP menjadi kritis dalam

menghubungkan kampus-kampus yang menggunakan AS yang berbeda. Sebagai contoh, Kampus I menggunakan AS 100 sementara Kampus II menggunakan AS 200. Implementasi *routing protocol* BGP diterapkan untuk memungkinkan kedua kampus saling terhubung dan berinteraksi satu sama lain.

Penelitian Paramartha, dkk. [11] tahun 2016 dilakukan penelitian yang berfokus pada implementasi jaringan *multihoming* menggunakan *routing protocol* BGP di Fakultas Hukum Universitas Udayana (UNUD). Dimana Fakultas Hukum memiliki koneksi ke GDLN Udayana sebagai jalur utama untuk terhubung ke internet. Namun, jika terjadi gangguan atau pemutusan koneksi pada jalur GDLN, akses internet menjadi terganggu. Sehingga Fakultas Hukum memutuskan untuk menerapkan jaringan *multihoming* menggunakan BGP agar tetap dapat terhubung ke internet melalui jalur alternatif, yaitu jalur ISP, jika terjadi masalah pada jalur GDLN. Dalam penelitian ini, teridentifikasi suatu kelemahan, yaitu keterbatasan fokus pada penggunaan hanya dua *gateway* sebagai akses ke internet. Oleh karena itu, disarankan untuk menambahkan lebih banyak *gateway* sebagai rute keluar tambahan. Dengan demikian, jaringan komputer Fakultas Hukum UNUD dapat mengatasi gangguan pada jalur utama dengan lebih baik dan tetap memiliki akses internet yang stabil melalui jalur alternatif ketika diperlukan.

Penelitian ini memiliki perbedaan yang signifikan dari penelitian sebelumnya karena memfokuskan pada implementasi *routing protocol* BGP dan melakukan perbandingan antara dua metode BGP, yaitu *Dual Homed* dan *Single Multihomed*. Penelitian ini juga menganalisis perbedaan kinerja antara kedua metode tersebut menggunakan parameter QoS seperti *throughput, packet loss, delay*, dan *jitter*. Pada Tabel 2.1 ditunjukan mengenai keterkaitan penelitian ini dengan penelitian sebelumnya.

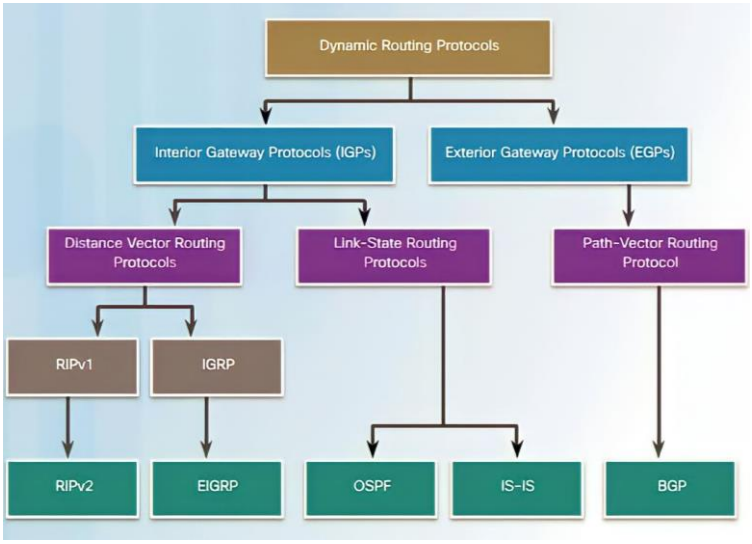
Tabel 2.1 Rangkuman Keterkaitan Dengan Penelitian Sebelumnya.

Peneliti	Judul Penelitian	Penelitian Utama
Putra, dkk	Analisis Perbandingan Kinerja Metode *Single Homing* dan *Multihoming* dengan Protokol *Border Gateway Protocol* (BGP	Dalam penelitian ini, digunakan *routing protocol* BGP sebagai protokol pengaturan rute jaringan. Penelitian ini berfokus pada pengujian parameter QoS

Peneliti	Judul Penelitian	Penelitian Utama
		dan waktu konvergensi. Pengujian QoS dilakukan dengan mengukur nilai *delay* dan *packet loss* menggunakan ICMP. Selain itu, penelitian ini juga melakukan perbandingan efektivitas antara metode *single homing* dan *multihoming* dalam pengaturan rute jaringan.
Musril	Simulasi Interkoneksi Antara *Autonomous System* (AS) Menggunakan *Border Gateway Protocol* (BGP)	Protokol yang digunakan dalam penelitian ini adalah *Border Gateway Protocol* (BGP). parameter pengujian yang digunakan adalah konektivitas antara perangkat dalam jaringan yang terhubung melalui BGP, protokol pengujian yang digunakan adalah ICMP untuk melakukan *traceroute* dan mengecek konektivitas antar perangkat dalam jaringan.
Paramartha, dkk	Penerapan Jaringan *Multihoming* Pada Jaringan Komputer Fakultas Hukum	Dalam penelitian ini, *Border Gateway Protocol* (BGP) digunakan sebagai protokol *routing*, dan metode *Multihoming* digunakan untuk mengimplementasikannya. Selain itu, protokol pengujian yang digunakan adalah ICMP untuk melakukan *traceroute*.

2.2 *ROUTING PROTOCOL*

Dua komponen penting utama dalam jaringan komputer adalah sumber dan tujuan. Informasi harus dikomunikasikan dari sumber ke tujuan dari waktu ke waktu. Ada banyak jalur yang digunakan di mana data dapat ditransfer. *Routing* merupakan proses pemilihan jalur terbaik atas jalur lainnya, *routing* dapat dilakukan oleh perangkat lunak yang di program yang dikenal sebagai protokol. Protokol standar membantu menemukan rute terbaik untuk memastikan transfer data yang baik. Paket data yang harus dikirim juga akan diberikan beberapa informasi untuk menemukan protokol *routing* yang terbaik. *Routing protocol* dibedakan menjadi 3 jenis yaitu *Default Routing*, *Static Routing*, dan *Dynamic Routing*. Tujuan utama dari *routing protocol* adalah untuk mengetahui tentang semua rute jaringan yang ada dan membuat keputusan yang benar. Pada *Dynamic Routing* dibag lagi menjadi 2 jenis yaitu *Interior Gateway Protocol* (IGP) dan *Exterior Gateway Protocol* (EGP) sesuai pada Gambar 2.1 [12].



Gambar 2.1 Jenis *Dynamic Routing Protocol*.

Interior Gateway Protocol (IGP) digunakan untuk menghubungkan jaringan yang berada dalam satu AS yang sama. IGP terdiri dari 2 jenis yaitu *Link-State Routing* dan *Distance Vector Routing*. Pada *Link-State Routing* terdiri dari 2 *routing protocol* yaitu *Open Shortest Path First* (OSPF) dan *Intermediate System to Intermediate System* (IS-IS). Sedangkan pada *Distance Vector Routing* terdiri dari 4 *routing protocol* yaitu *Routing Information Protoocol* (RIP) *version*1, RIPv2,

Enhanced Interior Gateway Routing Protocol (EIGRP), dan *Interior Gateway Protocol* (IGRP) [13].

Protokol EGP menyediakan konektivitas antara AS yang berbeda. Karena AS yang berbeda milik entitas administratif yang berbeda, administrator tidak dapat menggunakan protokol perutean pilihan mereka untuk menghubungkannya. Saat ini, BGP adalah satu-satunya protokol perutean eksterior yang digunakan. BGP menghubungkan semua sistem AS publik di internet [14].

2.3 *BORDER GATEWAY PROTOCOL* (BGP)

BGP adalah protokol yang berfungsi untuk menghubungkan antar AS yang berbeda. Ini mempertahankan informasi jalur dan secara dinamis memperbarui informasi dengan pembaruan tambahan. Untuk mempertahankan informasi jalur, BGP menggunakan tabel perutean terpisah [14]. BGP termasuk dalam kategori *routing protocol* jenis EGP yang digunakan untuk melakukan *routing* antar AS yang berbeda. BGP memungkinkan *router* untuk melakukan pertukaran rute yang ada dalam dan keluar dari jaringan lokal AS. Penggunaan BGP relevan ketika ingin menyewa IP Publik dari *registry* internet dan memiliki *Autonomous System Number* (ASN) sendiri. Selain itu, BGP digunakan ketika bertindak sebagai *Network Access Provider* (NAP) atau *Internet Service Provider* (ISP), saat memanipulasi lalu lintas data secara *downstream* atau *upstream*, dan saat memerlukan informasi jalur dari *prefix* internet. Ada dua versi BGP yaitu, IBGP dan EBGP. IBGP menyediakan perutean dalam AS yang sama. EBGP menyediakan perutean antara AS yang berbeda [15].

1. IBGP (*Interior Border Gateway Protocol*)

   IBGP digunakan untuk mengalihkan rute di dalam AS yang sama. Sebagai salah satu "*Interior Routing Protocol*", IBGP memiliki peran penting dalam melakukan *routing* aktif di dalam suatu jaringan. Protokol ini bekerja bersama dengan *Interior Gateway Protocol* (IGP) dan *Internal* BGP (IBGP) untuk memastikan tercapainya *routing* intradomain secara efektif. IGP membangun konektivitas untuk *prefix* internal, IBGP digunakan untuk menentukan *gateway* keluar untuk paket-paket yang tujuannya berada di luar AS. Di IBGP, tidak ada batasan bahwa *neighbor* harus terhubung secara langsung [16]. Setiap *router* BGP harus memiliki koneksi dengan IBGP (*Internal* BGP) di dalam satu AS

yang sama untuk mencapai interkoneksi antara satu *router* dengan *router* lainnya di seluruh jaringan. Contohnya ketika sebuah *router* BGP A menerima *routing information* dari salah satu *router* BGP B *neighbor* dalam satu AS yang sama, *router* BGP A tidak akan mengrimkan *routing information* ke *router* BGP yang lain yang terhubung agar tidak terjadi *routing loop*. IBGP mempunyai kelemahan yang besar karena nilai *Administrative Distance* (AD) bernilai 200 [17].

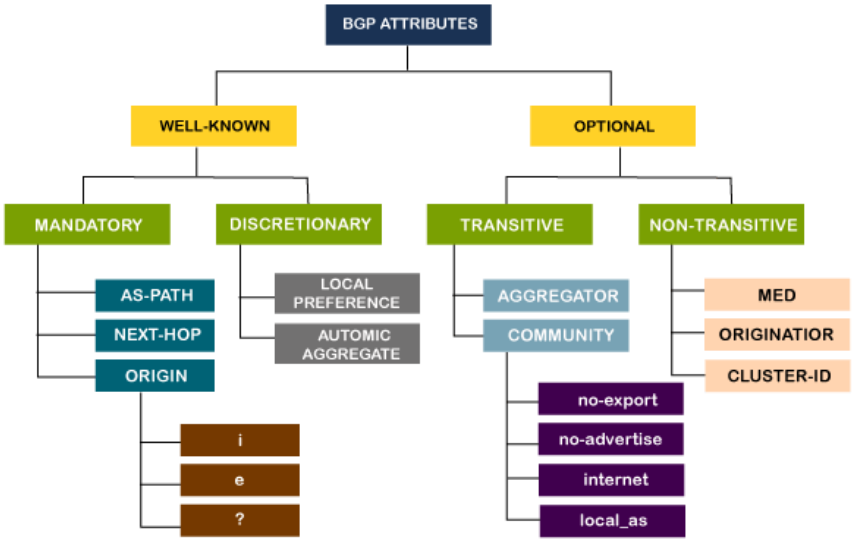
2. EBGP (*Exterior Border Gateway Protocol*)

   External Border Gateway Protocol (EBGP) merupakan protokol *routing* antar domain yang digunakan untuk pertukaran informasi *routing* antara AS yang berbeda. Dalam konteks interkoneksi antar jaringan, setiap sistem otonom biasanya memiliki satu atau lebih *router* yang menjalankan perangkat lunak EBGP. EBGP selalu berusaha untuk mengumumkan setiap rute BGP yang diketahui ke semua pihak sehingga dari hal tersebut perlu adanya filter untuk mengendalikannya. EBGP menggunakan atribut yang selalu ada di setiap rute untuk menerapkan kebijakan perutean, dimana atribut tersebut digunakan untuk memilih jalur "terpendek" di beberapa AS, bersama dengan satu atau beberapa kebijakan perutean lainnya [18].

   Ketika hanya satu tautan yang menghubungkan dua AS, IP *address* dari *interface* yang terhubung digunakan untuk membuat sesi BGP antara keduanya. Dapat menggunakan IP *address* lain pada *interface*, tetapi alamat tersebut harus dapat dijangkau tanpa menggunakan konfigurasi IGP. Ketika menggunakan EBGP, terdapat persyaratan pokok yang harus terpenuhi untuk mengirimkan rute yang dimiliki oleh suatu AS melalui jaringan AS lain. EBGP mempunyai keuntungan yang besar karena nilai AD bernilai 20. AD merupakan tingkat kepercayaan dari sebuah sumber informasi rute. Semakin kecil nilai AD, makan semakin dipercaya untuk dipilih pertama dalam proses pemilihan rute terbaik [19].

Routing protocol BGP memiliki keunikan yang terletak pada atribut pendukungnya. BGP menggunakan sekumpulan atribut untuk menentukan jalur terbaik untuk setiap tujuan dan untuk mengatur pertukaran informasi *routing* antara *router* BGP yang bertetangga. Atribut-atribut ini dapat dibag lagi menjadi empat

kategori berbeda yaitu *Well-known Mandatory*, *Well-known Discretionary*, *Optional Transitive*, *Optional Non-Transitive*. Pemilihan jalur BGP dilakukan melalui algoritma jalur terbaik. Jika BGP berisi beberapa rute ke tujuan yang sama, BGP berturut-turut menganalisis atau membandingkannya untuk menentukan jalur mana yang paling efisien untuk diambil atau biasa disebut *BGP Best Path*. Dimana ada 11 jenis atribut yang mepunyai fungsi yang berbeda dan ciri khas tersendiri untuk melakukan manajemen dalam *routing protocol* BGP. 11 atribut dibandingkan secara spesifik yaitu dengan menggunakan rute terbaik *Weight, Local Preference, Locally Orignated, AS path length, Orign code, Multiple Exit Discriminator (MED), eBGP path over iBGP path, Shortest IGP path to BGP next-hop, Oldest-path, Router ID, Neighbor IP address* [20]. Daftar jenis atribut BGP ditunjukan pada Gambar 2.2.



Gambar 2.2 Atribut BGP.

Pemilihan rute terbaik menuju ke tempat tujuan menggunakan algoritma *best path selection*. Dijelaskan sebagai berikut:

1. Memilih rute terbaik berdasarkan nilai *Weight* terbesar. Rute yang mempunyai nilai *Weight* terbesar akan prioritaskan pertama dipilih untuk rute terbaik dibandingkan nilai *Weight* terkecil.
2. Memilih rute berdasarkan nilai *LOCAL_PREF* yang paling tinggi. Rute dengan nilai *LOCAL_PREF* yang lebih besar akan mendapatkan prioritas lebih tinggi. Atribut ini digunakan untuk memilih rute yang lebih diutamakan daripada rute lain untuk *prefix* tujuan yang sama.

3. BGP memilih rute dengan *AS_PATH* terpendek. Dengan memprioritaskan *AS_PATH* yang paling pendek, BGP menganggap bahwa semakin singkat *AS_PATH*, semakin kecil *delay* yang akan terjadi. Ketika informasi *routing* disebarluaskan dalam jaringan, setiap ASN akan ditambahkan ke dalam *AS_PATH*.
4. Memilih rute terbaik berdasarkan nilai *ORIGN* yang terkecil. Rute yang nilai *ORIGN* terkecil lebih diprioritaskan untuk dipilih menjadi rute terbaik.
5. Memilih rute dengan nilai MED terkecil. MED ini digunakan untuk memilih *egress point* dalam domain lokal. Rute tanpa atribut MED dianggap memiliki MED terendah.
6. Memilih rute EBGP dibandingkan rute IBGP. Karena semakin kecil nilai AD, maka semakin besar kemungkinan untuk menjadi pilihan rute terbaik.
7. Menggunakan rute terbaik dengan nilai IGP *cost* terkecil menuju *BGP_NEXT HOP*. Tujuan dari langkah ini adalah untuk memastikan bahwa paket dapat segera meninggalkan domain atau wilayah AS yang lebih kecil. Hal ini dicapai dengan mengalihkan lalu lintas trafik ke BGP *router* terdekat berdasarkan nilai IGP *cost* yang lebih rendah. [21].

Pada dasarnya BGP memiliki *message* yang digunakan sebagai informasi untuk paket data, yang mana paket datanya dapat dikirimkan dengan baik atau tidak. 4 jenis *message* dari BGP yaitu:

1. *Open Message* adalah pesan pertama yang dikirim oleh setiap *router* BGP setelah sambungan protokol *transport* telah dibuat. Pesan ini digunakan untuk menetapkan penggunaan paket data TCP atau *User Datagram Protocol* (UDP) dan berfungsi sebagai inisiasi sesi komunikasi antar *router* BGP. Sebelum adanya *update message*, *notification message*, dan *keep alive message* dapat ditukarkan *open message* ini dikonfirmasikan terlebih dahulu menggunakan pesan *keep alive* yang dikirim oleh *router* BGP lainnya.
2. *Update Message* (pesan pembaharuan) dikirim menggunakan paket data TCP untuk memastikan kehandalan pengiriman. *Update Message* berfungsi untuk menyediakan pembaharuan informasi *routing* kepada *router* BGP lain, sehingga *router* dapat membangun pandangan yang konsisten tentang topologi

jaringan. Selain itu, pesan *update* juga digunakan untuk menarik beberapa rute yang tidak layak dari tabel informasi *routing.*

3. *Notification Message* (pesan pemberitahuan), dikirim saat terjadinya kondisi kesalahan terdeteksi. Berfungsi sebagai penutup sesi aktif dan mengnformasikan kepada *router* BGP lain yang terhubung dimana sesi aktifnya ditutup. *Notification message* ini beridi *field-field* tentang *error* yang terjadi, sehingga memudahkan pengguna dalam melakukan *troubleshooting*.
4. *Keep Alive Message*, dikirim kepada *router* BGP lain dimana agar sesi antar *router* BGP tidak mengalami *expired* atau kadaluwarsa. Pesan ini berfungsi untuk memberitahukan kepada *router* BGP agar *router* tersebut selalu *on* dan tidak pernah *down* [7].

2.4 *AUTONOMOUS SYSTEM* (AS)

Autonomous System (AS) merupakan sekumpulan jaringan yang berada dibawah kontrol satu atau sistem administrasi dan memiliki *routing policy* yang sama. Biasanya sekumpulan *router* tersebut dimiliki oleh perusahaan/organisasi yang sama seperti: *service provider*, kampus, perusahaan, dll. Dalam satu AS, beberapa *router* di dalamnya dapat saling berkomunikasi dan saling mengrimkan informasi, dan untuk bertukar informasi *routing* dalam satu AS harus menggunakan *routing protocol* yang sama [15]. Biasanya, sistem ini menggunakan sebuah Protokol *Gateway Interior* (*Interior Gateway Protocol*/IGP). Penetapan sistem otonom (AS) diperlukan ketika suatu jaringan terhubung ke lebih dari satu AS yang memiliki kebijakan *routing* yang berbeda. Dengan adanya pembagian AS, jaringan besar dapat diatur secara lebih terstruktur dan mengikuti kebijakan *routing* yang telah ditentukan dengan jelas.

Untuk membedakan satu AS dengan AS lain, maka setiap AS diidentifikasi oleh AS *Number*. Nomor tersebut diatur oleh internet *Assigned Numbers Authority* (IANA). IANA memiliki beberapa organisasi dibawahnya dan Indonesia tergabung dalam organisasi *Asia Pasific Network Information Center* (APNIC). AS *number* memiliki ukuran 16 *bit*. Pemberian nomor AS untuk 2 *bytes* AS *number range*: 0 - 65.535 dan untuk 4 *bytes* AS *number range*: 65.536 - 4.294.967.295. AS dibedakan menjadi 2 jenis yaitu *private* dan *public* AS, *private* AS bisa digunakan ketika kita menggunakan satu *service provider* dan mengngnkan *routing policy* antara AS yang

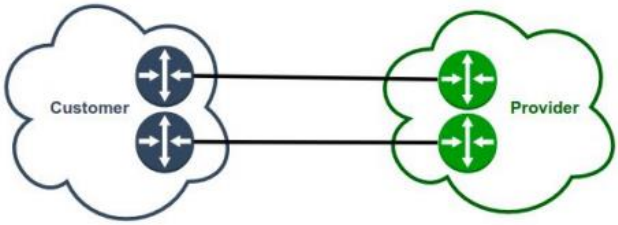
digunakan dengan AS *service provider* tidak terlihat dari internet. *Range private* AS 2 *bytes*: 64512 - 65534 dan *range private* AS 4 *bytes*: 4200000000 – 4294967294. Sedangkan pada *public* AS *number*, nomor AS berada diantara 1 sampai 65535 [22].

2.5 *DUAL HOMED*

Dalam koneksi *Dual-Homed Network*, sebuah *link* memiliki dua atau lebih koneksi ke ISP atau NAP yang sama. *Dual-homed* dapat dihubungkan ke satu atau dua *router* ISP atau NAP di mana satu tautan adalah *primer* dan yang lainnya sekunder atau cadangan. Cara lain POP dapat menggunakan topologi ini adalah dengan memuat keseimbangan lalu lintas menggunakan kedua tautan. Jenis jaringan ini juga menawarkan redundansi *link* di sisi *host*. Pada Gambar 2.3 bisa dilihat seperti apa koneksi jaringan *dual-homed.* Kelemahan lain dari metode *dual-homed* pada Gambar 2.3 yaitu melibatkan dua *router* ISP atau NAP terpisah dari ISP atau NAP yang sama. Ini kemungkinan besar akan meningkatkan biaya solusi [23].

Gambar 2.3 Topologi Jaringan *Dual-Homed*.

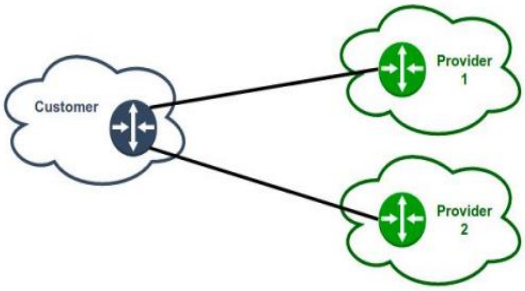
Pada koneksi tautan *link dual-homed* menambahkan beberapa redundansi. *Link* masih terhubung ke satu ISP atau NAP, tetapi apabila menggunakan dua tautan, bukan hanya satu tautan saja. Ada beberapa variasi untuk desain *dual-homed*. Pada Gambar 2.4 merupakan variasi dari desain *dual-homed*. Yang mana menawarkan redundansi paling banyak saat terhubung ke satu ISP atau NAP. Berdasarkan Gambar 2.4 memiliki dua tautan *link* dan dua *router* di kedua ujungnya. Salah satu kelemahan dari desain ini adalah masih menggunakan ISP tunggal dan juga kemungkinan besar akan lebih mahal, karena *customer* membeli konektivitas kedua ISP atau NAP berbeda, jadi tidak dapat memanfaatkan diskon apa pun yang mungkin diberikan satu ISP atau NAP kepada untuk beberapa tautan [24].



Gambar 2.4 Variasi Topologi Jaringan *Dual-Homed*.

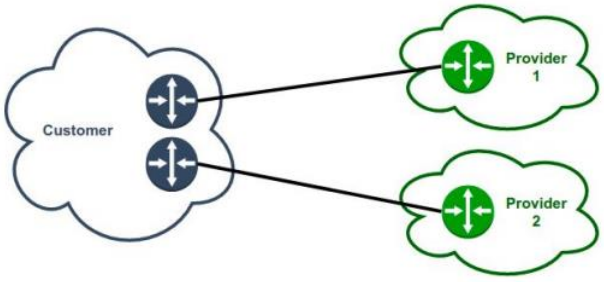
2.6 *SINGLE MULTIHOMED*

Multihomed merupakan sebuah metode jaringan yang terkoneksi dengan minimal dua ISP yang berbeda. Topologi *single-multihomed* berarti memiliki lebih dari satu jalur keluar untuk terhubung ke internet dengan menggunakan lebih dari satu ISP yang berbeda. Ditampilkan pada Gambar 2.5 yang menunjukan topologi jaringan dari *single-multihomed,* berdasarkan gambar tersebut dapat dilihat hanya memiliki satu *router* di pelanggan, terhubung kedua ISP yang berbeda. Satu-satunya titik kegagalan dalam desain ini adalah hanya memiliki satu *router* di pelanggan. Jika gagal, sudah tidak akan dapat terhubung ke ISP mana pun.



Gambar 2.5 Topologi Jaringan *Single-Multihomed*.

Pada Gambar 2.6, merupakan variasi desain dari topologi jaringan *single-multihomed,* desain tersebut cukup bagus untuk dioperasikan nantinya, pada desain tersebut hanya menggunakan tautan *link* tunggal, tetapi terhubung kedua ISP yang berbeda dengan menggunakan *router* berbeda juga.



Gambar 2.6 Variasi Topologi Jaringan *Single-Multihomed*.

2.7 *QUALITY OF SERVICE* (QOS)

Quality of Service (QoS) merupakan suatu arsitektur *end-to-end* dan bukan sekadar sebuah fitur terpisah dalam jaringan. Dalam konteks jaringan, QoS merujuk pada tingkat kecepatan dan kehandalan penyampaian berbagai jenis data dalam suatu komunikasi. QoS merupakan QoS yang berorientasi pada jaringan yang bersangkutan apa yang jaringan tersebut dapat lakukan untuk aplikasi. QoS merupakan kualitas layanan jaringan yang di dapat melalui:

1. Desain teknis jaringan adalah proses yang menentukan karakteristik koneksi yang melewati jaringan.
2. Kondisi akses jaringan, terminasi, dan *link* antar *switch* merupakan faktor-faktor yang menentukan apakah suatu jaringan memiliki kapasitas yang cukup untuk mengatasi semua permintaan pengguna.

Dalam kata lain, QoS dapat dijelaskan melalui parameter-parameter kinerja jaringan seperti *latency*, *delay*, *throughput, packet loss*, dan lain-lain [25]. Tingkat kualitas jaringan disesuaikan dengan standar QoS melalui tabel yang dikeluarkan oleh TIPHON.

1. *Throughput*

   Throughput merupakan kecepatan pemrosesan sesuatu yang biasa disebut dengan *bandwidth actual* dari suatu sistem untuk mengrim data ke yang lain, dengan menghitung faktor tambahan. Berdasarkan pada jaringan komunikasi, *throughput* merupakan tingkat pengriman pesan melalui satu saluran. *Throughput* menampilkan hasilnya sebagai ratarata dan menggunakan metrik seperti “bps” atau “pps". *Throughput* berbeda dengan *bandwidth*, *bandwidth* merupakan kapasitas total dari suatu sistem untuk mengrim data ke yang lain melalui satu media, sedangkan *throughput* memberi tahu berapa banyak data yang ditransfer dari sumber pada waktu tertentu dan *bandwidth* memberi tahu berapa banyak data yang secara teoritis dapat ditransfer dari sumber pada waktu tertentu. Rumus 2.1 menjelaskan tentang perhitungan nilai. Pada tabel 2.2 menunjukan tabel kategori *throughput* menurut stsandar TIPHON [26].

Tabel 2.2 Kategori *Throughput* Berdasarkan Standar TIPHON.

Kategori *Throughput*	Besar *Throughput*
Sangat Baik	>2,1 Mbps
Baik	1200 Kbps - 2,1 Mbps
Cukup	700 – 1200 Kbps
Buruk	0 – 338 Kbps

$$Throughput = \frac{\text{Paket yang diterima}}{\text{Lama pengamatan}} \quad (2.1)$$

2. *Delay*

Delay merupakan keterlambatan dalam waktu transmisi data dari pengrim dan penerima, satuan dari *delay* adalah sekon (detik). *Delay* dapat dipengaruhi oleh jarak media fisik, kemacetan *traffic* jaringan, atau lama waktu pemrosesan. *Delay* juga merupakan penundaan waktu pulang pergi dimana waktu yang diperlukan untuk mengrim paket dari komputer ke komputer tujuan. Penundaan yang berarti lamanya waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Jika waktu yang dibutuhkan untuk mengrimkan paket dari *host* ke media transmisi disebut *tansmission delay*. Rumus 2.2 menjelaskan tentang perhitungan nilai. Pada tabel 2.3 menjelaskan standar kategori *delay* berdasarkan TIPHON [26].

Tabel 2.3 Kategori *Delay* Berdasarkan Standar TIPHON.

Kategori *Delay*	*Delay* (ms)
Sangat Baik	<150 ms
Baik	150 ms – 300 ms
Cukup	300 ms – 450 ms
Buruk	>450 ms

$$\text{Rata} - \text{rata } delay = \frac{\text{Total } delay}{\text{Total paket yang diterima}} \quad (2.2)$$

3. *Packet loss*

Packet loss merupakan persentase dari suatu paket yang hilang selama transmisi data. Yang disebabkan oleh banyak faktor, seperti sebagai penurunan sinyal dalam jaringan, kesalahan *hardware* jaringan, atau radiasi dari lingkungan sekitarnya. *Packet loss* berarti jumlah paket yang gagal mencapai tujuan dikirim. Pada protokol paket data seperti TCP yang bersifat *connection oriented*, yang menyediakan pengriman kembali (*retansmission*) saat paket data yang hilang selama proses tansmisi data. Walaupun TCP memiliki kelebihan tersebut, jika TCP melakukan *retransmitting* atau *resends*, nilai *throughput* semakin menurun. Berbeda halnya dengan protokol UDP yang memiliki sifat *connectionless*, tidak menyediakan pengriman kembali ketika kehilangan paket data selama proses transmisi data. Rumus 2.3 menjelaskan tentang perhitungan nilai *packet loss*. Tabel 2.4 menjelaskan kategori *packet loss* berdasarkan standar TIPHON [26].

Tabel 2.4 Kategori *Packet Loss* Berdasarkan Standar TIPHON.

Kategori *Packet loss*	*Packet loss* (%)
Sangat Baik	0%
Baik	3%
Cukup	15%
Buruk	25%

$$Packet\ loss = \frac{\text{Paket data dikirim} - \text{Paket data diterima}}{\text{Paket data yang dikirim}} \text{ X } 100\% \qquad (2.3)$$

4. *Jitter*

Jitter adalah istilah yang digunakan dalam jaringan komputer untuk menjelaskan ketidakteraturan dalam waktu yang diperlukan oleh paket data untuk sampai ke tujuan mereka. Dalam kata lain, *jitter* menggambarkan variasi atau perbedaan waktu kedatangan paket data saat dikirim melalui jaringan. *Jitter* dapat dijelaskan sebagai perbedaan antara waktu kedatangan paket data yang paling cepat dengan waktu kedatangan paket data yang paling lambat dalam kelompok paket yang dikirim melalui jaringan. Dengan kata lain, *jitter* mencerminkan variasi waktu yang terjadi saat paket data diterima, di mana

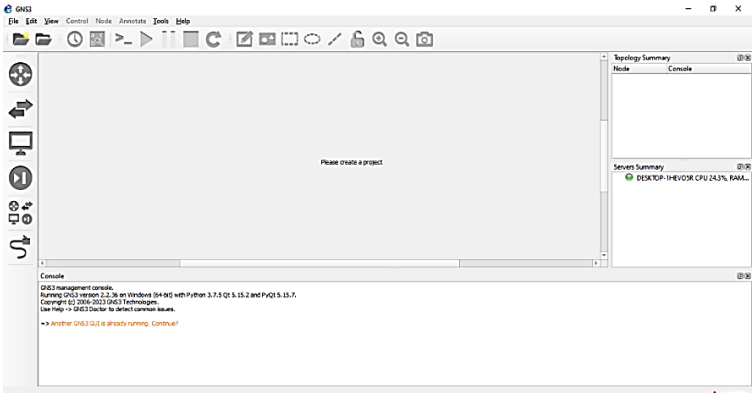
beberapa paket datang lebih cepat sedangkan yang lain datang lebih lambat dalam satu kumpulan paket yang dikirim melalui jaringan [28].

Tabel 2.5 Kategori *Jitter* Berdasarkan Standar TIPHON.

Kategori *Jitter*	*Jitter*
Sangat Baik	0 ms
Baik	0 ms – 75 ms
Cukup	76 ms – 125 ms
Buruk	125 ms – 225 ms

2.8 *GRAPICHAL NETWORK SIMULATOR (*GNS3)

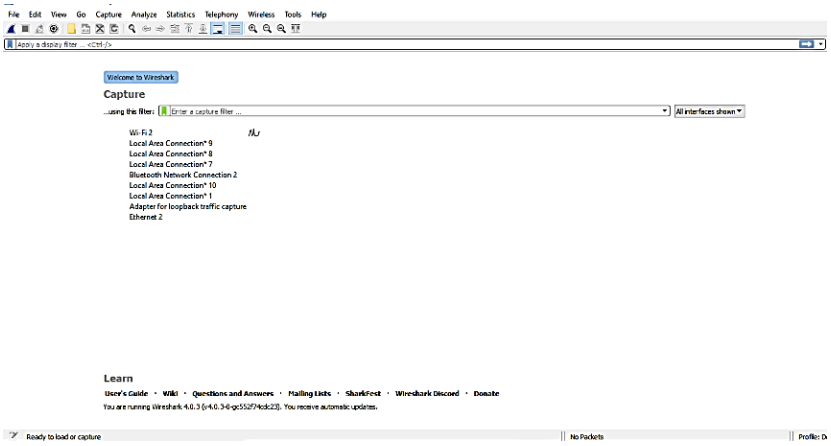
Grapichal Network Simulator **(**GNS3) merupakan aplikasi simulator jaringan grafis atau *Graphical User Interface* (GUI) yang memungkinkan untuk mensimulasikan jaringan virtual lebih dari 20 produsen yang berbeda pada komputer lokal, dengan memasang virtual jaringan ke jaringan nyata atau disebut juga dengan virtualisasi [29]. GNS3 adalah sebuah platform simulasi jaringan yang memungkinkan pengguna untuk melakukan simulasi jaringan yang kompleks. Keunggulan GNS3 terletak pada penggunaan sistem operasi asli dari perangkat jaringan (*closed source*) seperti *router* Cisco, Juniper, Mikrotik, dan *Virtual Machine*. Dengan menggunakan sistem operasi asli, peneliti dapat melakukan konfigurasi alat secara langsung dalam kondisi yang lebih mendekati keadaan nyata, dibandingkan dengan penggunaan Cisco *Packet Tracer*. GNS3 dipakai untuk simulator *switch* tentunya yang *manageble* seperti *switch* Cisco. Gambar 2.7 menunjukan tampilan GNS3 [30].



Gambar 2.7 Tampilan GNS3.

2.9 *WIRESHARK*

Wireshark adalah perangkat lunak *open-source* yang berfungsi untuk memindai dan merekam lalu lintas jaringan internet. Aplikasi ini sering digunakan dalam *troubleshooting* jaringan yang mengalami masalah dan juga dalam pengujian perangkat lunak karena kemampuannya dalam membaca isi setiap paket data yang dikirimkan dan diterima dalam jaringan. *Wireshark* sangat berguna untuk menganalisis suatu jaringan. Untuk cara kerjanya dengan *capture* paket data dari berbagai protokol dengan berbagai jenis jaringan yang biasa ditemukan dalam *traffic* internet. Paket data yang telah diambil kemudian dipresentasikan dalam jendela tampilan hasil penangkapan waktu nyata. Pada Gambar 2.8 menunjukan tampilan *Wireshark* [30].



Gambar 2.8 Tampilan *Wireshark*.

2.10 *INTERNET CONTROL MESSAGE PROTOCOL* (ICMP)

Packet Internet Gopher (PING) merupakan suatu fitur yang memiliki peran utama dalam melakukan pengecekan komunikasi antar host dalam sebuah jaringan. Fitur PING ini beroperasi di bawah protokol *Internet Control Message Protocol* (ICMP) yang berfungsi untuk mengirimkan pesan *echo request* kepada alamat IP *host* tujuan, kemudian menunggu dan meminta balasan dari *host* tujuan sebagai respons atas permintaan tersebut [31].

2.11 *SECURE SHELL FILE TRANSFER PROTOCOL* (SFTP)

Secure File Transfer Protocol (SFTP) adalah protokol transfer *file* yang aman dan berbasis pada *Secure Shell* (SSH). SFTP memungkinkan pengguna untuk

mentransfer *file* secara aman antara komputer lokal dan *server* jarak jauh melalui enkripsi data. Dengan menggunakan SFTP, data yang dikirimkan antara perangkat dikodekan, sehingga melindungi informasi dari potensi ancaman keamanan. SFTP sering digunakan untuk akses dan mengelola *file* di *server* secara efisien dan aman melalui koneksi yang dienkripsi [32].