BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian Vico Andrea Budi Harto, Rakhmadhany Primananda, Aswin Suharsono pada tahun 2017 yang berjudul "Analisis Performansi H.264 dan H.265 pada *Video Streaming* dari segi *Quality of Service*" meneliti tentang mengetahui perfromansi QoS layanan video streaming menggunakan *codec* kompresi H.264 dan H.265. Pengujian dilakukan untuk mengetahui efek penggunaan metode kompresi menurut ukuran *bitrate*, *framerate*, dan *bandwidth* yang digunakan. H.264/AVC merupakan *codec* video yang memiliki keunggulan dibanding *codec* video lain dengan kemampuan untuk *encoding* video dengan menekan *bitrate* pada video agar video yang dihasilkan lebih minim daripada video aslinya. H.265/HEVC merupakan video *codec* yang dikembangkan setelah H.264, bertujuan untuk mengefisiensikan *bitrate* video dengan mengompres *bitrate* dua kali lebih baik agar menghasilkan ukuran video yang lebih minim dengan kualitas yang sama dengan aslinya. Nilai *delay streaming live* H.264 dan H.265 adalah 18.04 ms dan 26.47 ms, ketika *store* adalah 8.47 dan 8.60 ms. Dapat disimpulkan performa H.264 dan H.265 dikarenakan memiliki nilai durasi yang lebih rendah, *throughput* yang lebih tinggi, dan *delay* yang lebih kecil [4].

Penelitian Laufi Deodo Saputra, Wiwin Sulistyo pada tahun 2017 yang berjudul "ANALISIS QOS *DIFFERENTIATED SERVICE* PADA JARINGAN MPLS MENGGUNAKAN ALGORITMA *THRESHOLD*" membahas mengenai performansi QoS pada jaringan MPLS menggunakan algoritma *threshold* dengan teknologi IETF (*Internet Engineering Task Force*). Untuk memenuhi permintaan QoS diantaranya adalah penggabungan teknologi MPLS *Diffserv* yang mampu mengklasifikasi paket sesuai kebutuhan, tetapi ketika penumpukan terjadi akibat proses QoS ini, paket yang menumpuk akan di-*drop*. Solusi untuk mengantisipasi *dropping* digunakanlah algoritma *threshold* pada WRED. Penambahan WRED sebagai

algoritma *threshold* pada jaringan MPLS *Diffserv* memberikan pengaruh untuk layanan VoIP yang mampu mengurangi *packet loss* 43,1%, delay 0,005% memaksimalkan *throughput* 1,26% dan mengurangi *jitter* 48,56% dan untuk layanan *video streaming* mengurangi *packet loss* 15,93% dan memaksimalkan throughput 1,6% dibanding sebelum menggunakan alhotirma *threshold* [5].

Penelitian Ahmad Akmaludin, Arini MT, Siti Umi Masruroh, M.Sc pada tahun 2019 yang berjudul "Evaluasi Kinerja *Hot Standby Router Protocol* (HSRP) dan *Gateway Load Balancing Protocol* (GLBP) untuk Layanan *Video Streaming*" membahas mengenai bagaimana jaringan dapat menangani kegagalan (*failure*) pada jaringan komputer yang mempengaruhi *Quality of Services* (QoS). Dalam jaringan internet, jalur cadangan (*redundant*) selalu ditambahkan untuk melengkapi jalur utama. Sehingga apabila jalur utama terganggu, lalu lintas data dapat dialihkan ke jalur cadangan, proses ini disebut dengan *network redundancy*. Ada dua *protocol* yang termasuk dalam FHRP yaitu *Hot Standby Routing Protocol* (HSRP), dan *Gateway Load Balancing Protocol* (GLBP). Dari kedua *protocol* HSRP dan GLBP akan dibahas manakah yang lebih baik dari kedua *protocol* tersebut untuk digunakan sebagai *network redundancy*. Hasil dari penelitian ini memberikan nilai QoS terbaik untuk nilai delay adalah ROUTER *protocol* HSRP, dan untuk nilai *Packet Loss* adalah HSRP, dan untuk nilai *throughput* adalah HSRP dan routing yang tepat untuk jaringan layanan *video streaming* adalah HSRP [1].

2.2 DASAR TEORI

2.2.1 INTERNET PROTOCOL

TCP/IP (*Transfer Control Protocol*/*Internet Protocol*) merupakan sebuah *protocol* yang digunakan pada jaringan internet. Pada protocol TCP/IP terdapat 2 bagian, yaitu TCP dan UDP serta lapisan yang ada dibawah bagian tersebut terdapat *protocol* yang disebut dengan IP. TCP (*Transmission Control Protocol*) merupakan protocol yang menjaga reliabilitas hubungan komunikasi antara *end-to-end*. Cara kerja TCP adalah mengirim dan

menerima segmen-segmen informasi dengan panjang data yang bervariasi pada suatu *datagram* internet. UDP (*User Datagram Protocol*) merupakan salah satu *protocol* utama diatas IP, yang lebih sederhana dibandingkan dengan TCP [6].

2.2.2 OSI *LAYER*

Open System Interconnection (OSI) diciptakan oleh ISO (*International Organization Standardization*) untuk menyediakan logika terstruktur proses komunikasi data melalui jaringan. Terdapat 7 *layer* pada OSI dan memiliki fungsi disetiapnya, yaitu:

1. *Physical Layer*

   Layer ini berfungsi untuk proses data menjadi *bit* dan mentransfer melalui media. Pada *layer* ini dapat mendefinisikan transmisi jaringan, metode pensinyalan, sinkronisasi *bit*, arsitektur jaringan, topologi jaringan.
2. *Data Link Layer*

   Layer ini menyediakan *link* untuk data dan memaketkannya menjadi *frame*. *Error coreection, flow control* dan pengalamatan (MAC *address*) akan di deteksi pada *layer* ini.
3. *Network Layer*

   Layer ini bertanggung jawab untuk menentukan alamat jaringan, menentukan rute, dan menjaga trafik di jaringan. Format yang digunakan pada layer ini adalah paket.
4. *Transport Layer*

   Pada *layer* ini data akan dipecah menjadi beberapa paket dan diberikan nomor urut di setiap paketnya, sehingga paket-paket tersebut dapat disusun kembali menjadi data awal yang dikirimkan. Bentuk data pada *layer* ini adalah segmen.
5. *Session Layer*

   Pada *layer* ini menentukan bagaimana menjaga, memelihara dan mengatur koneksi.

6. *Presentation Layer*

   Merupakan *layer* yang berfungsi untuk mengubah data yang akan di kirimkan ke jaringan oleh aplikasi ke dalam bentuk data yang dapat ditransmisikan melalui jaringan.

7. *Application Layer*

   Layer ini berfungsi untuk menghubungkan aplikasi dengan jaringan, mengatur aplikasi agar dapat mengakses jaringan, dengan kata lain, layer ini merupakan yang berhubungan langsung dengan *user* [7].

2.2.3 ROUTING

Routing adalah proses menentukan rute dari *host* asal ke *host* tujuan. *Routing* merupakan proses memindahkan data dari satu *network* ke *network* lain dengan cara mem-*forward* paket data *via gateway*. *Routing* menentukan kemana datagram akan dikirim agar mencapai tujuan. Sebuah *router* mempelajari informasi *routing* dari mana sumber dan tujuannya yang kemudian ditempatkan pada tabel *routing*. *Router* akan berpatokan pada tabel ini, untuk memberitahu *port* yang akan digunakan untuk meneruskan paket ke alamat tujuan [8].

2.2.4 *Open Shortest Path First* (OSPF)

OSPF bekerja berdasarkan algoritma *Shortest Path First* yang dikembangkan berdasarkan algoritma Dijkstra. Sebagai *Interior Gateway protocol* (IGP). *Interior Gateway protocol* atau *Interior Routing* Protokol dikembangkan untuk menghubungkan router-router dibawah kendali administrator jaringan. OSPF mendistribusikan informasi *routing*nya di dalam *router - router* yang tergabung kedalam suatu AS. AS adalah jaringan yang dikelola oleh administrator setempat. OSPF menggunakan protokol *routing link state*, didesain untuk bekerja dengan sangat efisien dalam proses pengiriman *update* informasi rute. OSPF merupakan *protocol alternative* untuk menutupi kelemahan RIP. OSPF ialah *protocol routing* yang menggunakan prinsip *multipath* dapat mempelajari berbagai rute dan memilih lebih dari satu rute ke *host* tujuan. OSPF digunakan bersama dengan IP, maksudnya paket OSPF dikirim bersamaan dengan *header* paket data IP. Setiap *router* OSPF mempunyai database identik yang menggambarkan

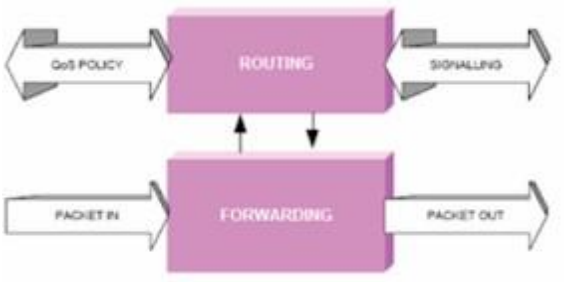
topologi suatu *Autonomous System* yang disebut dengan *Link State database* (*Topological database*). Dari *database* ini, perhitungan *Shortest Path First* dilakukan untuk membentuk *Routing* Tabel [9].

2.2.5 *Multi Protocol Label Switching* (MPLS)

MPLS adalah teknologi penyampaian paket pada jaringan *backbone* berkecepatan tinggi. Asas kerjanya menggabungkan beberapa kelebihan dari system komunikasi *circuit-switched* dan *packet-switched* yang melahirkan teknologi yang baik dari keduanya. MPLS adalah arsitektur *network* yang didefinisikan oleh IETF (*Internet Engineering Task Force*) untuk memudahkan mekanisme label *swapping* di layer 2 dengan routing di layer 3 untuk mempercepat pengiriman paket [10].

MPLS bekerja dengan cara memberikan label pada suatu paket data yang akan memasuki daerah *backbone* area, dari paket data tersebut akan menentukan rute dan prioritas pengiriman paket tersebut, dari label tersebut memuat suatu informasi penting yang berhubungan dengan informasi suatu *routing* paket, diantaranya berisi tujuan paket serta prioritas paket yang dikirimkan terlebih dahulu.

2.2.5.1 Arsitektur MPLS



Gambar 2. 1 **Arsitektur MPLS [10].**

Gambar 2.1 merupakan arsitektur MPLS. MPLS merupakan arsitektur network yang didefinisikan oleh IETF yang menggabungkan antara *label swapping layer* 2 dengan *routing layer* 3 untuk mempercepat pengiriman paket. Network MPLS terdiri atas *Label Switch Path* yang merupakan jalur yang melalui satu atau serangkaian *Label Switch Router*. Setiap LSP dikaitkan dengan sebuah *forwarding equivalence*

class yang merupakan kumpulan paket yang menerima dari *forwarding* yang sama di sebuah LSR. Untuk membentuk LSP, diperlukan suatu protokol persinyalan. Protokol ini menentukan *forwarding* berdasarkan label pada paket. Label yang pendek dan berukuran tetap mempercepat proses *forwarding* dan mempertinggi fleksibilitas pemilihan *path.* Hasilnya adalah *network* datagram yang bersifat lebih *connection-orriented* [10].

2.2.6 Gateway Load Balancing Protocol

First Hop Redundancy Protocol (FHRP) merupakan kelompok protokol yang memungkinkan router secara otomatis mengambil alih jika terjadi kegagalan pada router utama. Pengembangan dengan protokol ini terjadi biasanya dalam jaringan *Ethernet* dan *Token Ring*. Permasalahan terjadi ketika router utama mengalami kegagalan kemudian ada router kedua dalam segmen yang mampu menjadi *default gateway*. Sebab jika router utama gagal maka jaringan akan berhenti bekerja. Ada tiga solusi yaitu HSRP, VRRP, dan GLBP [11].

Gateway Load Balancing Protocol (GLBP) merupakan sebuah protokol yang hanya dimiliki oleh Cisco yang memiliki fungsi yang mirip dengan HSRP atau VRRP tetapi mendukung pembagian trafik dalam sebuah grup yang terhubung di GLBP. GLBP digunakan sebagai pembagi jaringan *dynamic* IP dengan *virtual gateway* dan *virtual MAC* dalam sebuah jaringan dengan *Load Balancing* [12]. GLBP memiliki 4 bagian yaitu:

a. *Active Virtual Gateway* (AVG) sebagai *gateway* yang aktif digunakan oleh jaringan dalam melakukan *request* data oleh seluruh *client*.
b. *Active Virtual Forwarder* (AVF) sebagai *forwarder* data yang telah di*request* oleh MAC tertentu. Setiap AVF melayani MAC tertentu sesuai pembagian *client* yang dilakukan AVG. *Load Balancing* terjadi ketika proses pembagian MAC dalam GLBP dilakukan dengan algoritma *Round Robin*, *Weighting*, atau *Hostdependent* [12].
c. *Virtual Gateway Redundancy*, sebagai router lain yang berperan sebagai *standby* AVG jika terjadi kegagalan pada AVG.

d. *Virtual Forwarder Redundacy*, sebagai router lain yang berperan sebagai *standby* AVF jika terjadi kegagalan pada AVF MAC tertentu [12].

2.2.7 Video Streaming

Video Streaming merupakan suatu layanan yang memungkinkan suatu server untuk mengirimkan *audio* dan *video* digital secara real time pada jaringan komputer. Layanan *video streaming* memungkinkan penggunanya untuk mengakses atau melihat suatu acara melalui komputer dari pengirim ke penerima. *Video Streaming* merupakan salah satu layanan yang banyak digunakan oleh masyarakat secara global, *Internet* telah menjadi media standar untuk pengiriman multimedia. Streaming menjadi media teknologi yang banyak digunakan dalam penerbitan berita multimedia, iklan secara *online*, e-*commerce, video on demand, tele-education, telemedicine* dan masih banyak aspek lain dari layanan informasi internet. Penerapan *streaming* sebagai media teknologi akan membawa perubahan besar pada pertukaran informasi jaringan dan memiliki dampak besar pada pekerjaan dan kehidupan manusia [13].

2.2.8 Format Video

Video analog mengenal beberapa format, antara lain: VHS, S-VHS, Beta, Hi-8. Sementara itu, video digital memiliki banyak sekali format, diantaranya yaitu, Digital 8, AVI, MOV, MPEG1 (VCD), MPEG2 (DVD) DV, MPEG4 (MP4), MKV dan lainnya. Perbedaan antar format yang satu dengan lainnya adalah ukuran rekaman gambar yang diberi istilah resolusi dan aliran data per detiknya yang disebut *data rate*. MPEG merupakan sistem yang mampu mengenali informasi yang sama antar-*frame*, lalu menghilangkannya. Hanya ada satu informasi saja yang digunakan sebagai acuan bagi *frame* - *frame* yang menggunakan informasi sama. Dengan cara itu, ukuran data jadi benar-benar berkurang dalam jumlah yang sangat berarti. Metode kompresi video dan audio sering kita dengar dengan julukan Codec (*Compressor Decompressor*) [21].

2.2.9 IP ADDRESS

Internet protocol addres atau dengan kata lain alamat IP merupakan sebuah kode atau identitas pengenal pada sebuah komputer di suatu jaringan. IP merupakan kode vital dalam jaringan internet, dikarenakan alamat IP merupakan identitas suatu perangkat untuk mengakses internet, maka pengalamatan IP antara satu alamat dengan alamat lainnya tidak boleh sama.

Sebelum dibuatnya *internet protocol*, pada jaringan memiliki peralatan dan *protocol* tersendiri yang di gunakan untuk saling berhubungan. Kemudian dibuatlah suatu *protocol* yang dapat digunakan secara umum dan dalam skala luas untuk dapat menyatukan berbagai perbedaan dalam penggunaan perangkat elektronik yang terhubung dalam jaringan internet. Protokol tersebutlah yang sampai saat ini masih banyak digunakan dan mendominasi dalam jaringan internet yaitu *internet protocol version* 4 (IPv4) [6].

2.2.10 IPV4

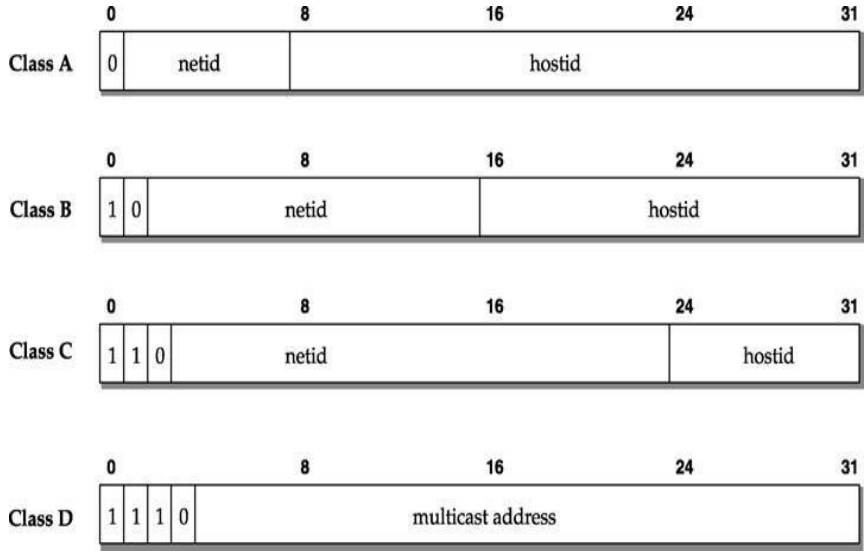
Alamat IPv4 merupakan sekumpulan bilangan biner sepanjang 32 *bit*, yang dibagi atas 4 segmen dan setiap segmen terdiri atas 8 *bit*. IP *address* merupakan identifikasi setiap *host* pada jaringan internet. Secara teori, tidak boleh ada dua *host* atau lebih yang tergabung ke internet menggunakan IP *address* yang sama. IP *address* dapat dipisahkan menjadi 2 bagian yaitu:

a. Bagian *network* (bit-bit *network*/*network* bit) atau disebut *network* ID.

b. Bagian *host* (bit-bit *host*/*host* bit) atau disebut *host* ID. Bit network berperan sebagai identifikasi *network*. Pada jaringan TCP/IP.

Perbedaan antar *network* tidak ditentukan dari jenis topologi, media fisik jaringan, luas area, jenis sistem operasi, aplikasi, dan sebagainya. Perbedaan jaringan dilihat dari bit-bit *network*. Sedangkan bit-bit *host* berperan dalam identifikasi *host* pada suatu *network*. Jadi, seluruh host yang tersambung dalam yang sama memiliki bit *network* yang sama namun bit *host*nya berbeda. Panjang bit *network* tidak selalu tetap, sangat bergantung kepada kelas *network* dan kondisi lain, seperti *subnetting* [14].

Untuk memudahkan pengaturan IP *address* seluruh komponen pengguna jaringan internet, dibentuklah suatu badan yang mengatur pembagian IP *address*. Badan tersebut bernama InterNIC (*Inter Network Information Center*) [14]. InterNIC membagi-bagi IP menjadi beberapa kelas seperti ditampilkan pada gambar 2.2 berikut:



Gambar 2.2 Struktur *classfull* IP *Address* [14].

Gambar 2.2 merupakan struktur dari *classfull* IP *address*, yang mana per-*class* akan dijelaskan sebagai berikut :

a. Kelas A

Jika *bit* pertama pada IP *address* adalah 0 maka IP *address* termasuk dalam kelas A. *Bit* ini dan 7 *bit* berikutnya (8 bit pertama) merupakan bit-bit *network* (*network* bit) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 24 *bit* berikutnya merupakan bit *host*. IP *address* harus dikonversikan dari benuk biner ke bentuk desimal.

b. Kelas B

Jika 2 *bit* pertama pada IP *address* adalah 10 maka IP address termasuk dalam kelas B. Dua *bit* ini dan 14 *bit* berikutnya (16 *bit* pertama) merupakan *bit-bit network* (*network* bit) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 24 *bit* berikutnya merupakan bit *host*.

c. Kelas C

Jika 3 *bit* pertama pada IP *address* adalah 110 maka IP *address* termasuk

dalam kelas C. Tiga bit ini dan 21 bit berikutnya (24 bit pertama) merupakan bit-bit *network* (*network* bit) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 8 *bit* berikutnya merupakan bit *host*.

d. Kelas D & E

Selain ketiga kelas diatas, ada 2 kelas lagi yang ditujukan untuk pemakain khusus, yaitu kelas D dan E. Jika 4 *bit* pertama adalah 1110, maka IP *address* termasuk dalam kelas D, IP *address* kelas D digunakan untuk multicast *address*. Selanjutnya kelas terakhir adalah kelas E, IP *address* kelas E digunakan untuk percobaan. Jika 4 *bit* pertama adalah 1111 (atau sisa dari seluruh kelas) maka IP *address* termasuk dalam kategori kelas E. Pemakaian IP *address* kelas E dicadangkan untuk kegiatan eksperimental [14].

2.2.11 ROUTER

Router merupakan perangkat keras jaringan komputer yang dapat digunakan untuk menghubungkan beberapa jaringan yang sama atau berbeda. *Router* adalah sebuah alat untuk mengirimkan paket data melalui jaringan atau internet untuk dapat menuju tujuannya, proses tersebut dinamakan *routing*. Proses *routing* itu sendiri terjadi pada lapisan 3 dari *stack* protokol tujuh-lapis OSI. Router terkadang digunakan untuk mengoneksikan 2 buah jaringan yang menggunakan media berbeda, seperti halnya dari Ethernet menuju ke *Token Ring*.

Router memiliki fungsi utama untuk membagi atau mendistribusikan *IP address*, baik itu secara statis ataupun DHCP atau *Dynamic Host Configuration Procotol* kepada semua komputer yang terhubung ke router tersebut. Dengan adanya *IP address* yang dibagikan *router* tersebut kepada setiap computer, maka dapat memungkinan setiap komputer untuk saling terhubung serta melakukan komunikasi, baik itu pada LAN atau internet. Untuk mendistribusikan *IP address* kepada setiap komputer pada suatu jaringan, fungsi *router* tidak saja hanya dapat menghubungkan dengan sambungan kabel LAN, melainkan dapat dengan teknologi *wireless* [15].

2.2.12 SWITCH

Switch adalah suatu komponen jaringan komputer yang berfungsi

untuk menghubungkan beberapa perangkat komputer agar dapat melakukan pertukaran paket, baik menerima, memproses, dan meneruskan data ke perangkat yang dituju. Pendapat lain mengatakan, pengertian *switch* adalah jenis komponen jaringan komputer yang digunakan untuk menghubungkan beberapa HUB dalam membentuk jaringan komputer yang lebih besar dan membutuhkan bandwidth yang cukup besar. Tidak seperti HUB, *switch* bekerja dengan lebih efisien, terarah, dan langsung pada alamat yang dituju, baik dalam pertukaran data, memproses, serta mengirim data. *Switch* dapat mendeteksi tujuan data sehingga dapat mencegah terjadinya 'tabrakan' pada saat data dikirim.

Fungsi *switch* dalam jaringan komputer adalah sebagai *concentrator* yang menerima dan membagikan data antar perangkat komputer. Adapun beberapa fungsi *switch* adalah sebagai berikut:

a. Address Learning

Switch mampu mencatat alamat MAC *address* dari suatu perangkat jaringan yang terhubung dengannya. Saat *switch* menerima data, *switch* akan mencatat MAC *address* pengirim dan mempelajari kemana data tersebut harus dikirim.

b. Meneruskan *Data Frame*

Switch juga dapat menyaring dan meneruskan suatu paket data yang diterima ke alamat tujuan, ke alamat MAC *address* dan *port* tujuan. Dengan begitu, maka proses pengiriman data tidak akan mengalami tabrakan.

c. Looping Avoidance

Switch mampu mencegah terjadinya *looping* (data hanya berputar pada *port switch*) ketika data yang diterima tidak diketahui tujuannya. Data yang diterima dapat diteruskan ke alamat tujuan dengan cara memblok salah satu *port* yang terhubung dengan perangkat lainnya.

Pada dasarnya cara kerja *switch* mirip seperti HUB, yang membedakan keduanya adalah kemampuan *switch* yang lebih baik dan efisien dalam pertukaran data, memproses, serta mengirim data. Pada praktiknya, *switch* akan menerima data dari perangkat lainnya yang terkoneksi dengannya. Lalu switch mendeteksi dan mencocokkan alamat MAC *Address* perangkat yang

dituju dengan data tabel yang dimilikinya. Selanjutnya, switch akan membuat suatu logika koneksi dengan *port* yang terhubung dengan perangkat tujuan. Dengan begitu, data yang dikirimkan hanya akan diterima oleh *port* yang dituju, sedangkan *port* lainnya tidak dapat menerima data tersebut.

Berdasarkan model OSI (*Open System Interconnection*), *switch* dapat dibedakan menjadi dua jenis, yaitu *Switch Layer* 2, beroperasi *Data Link layer* pada lapisan model OSI. Jenis *switch* ini dapat meneruskan paket data dengan mendeteksi MAC *Address* tujuan. Switch ini juga dapat melakukan fungsi *bridge* antara beberapa segmen LAN (*Local Area Network*) karena *switch* mengirimkan paket-paket data dengan cara melihat alamat yang dituju tanpa mengetahui protokol jaringan yang digunakan. *Switch Layer* 3, terdapat di *Network Layer* pada lapisan model OSI. Jenis *switch* ini dapat meneruskan paket data dengan menggunakan alamat IP suatu perangkat. Switch ini disebut juga dengan *switch routing* atau *switch multi-layer* [15].

2.2.13 KABEL LAN

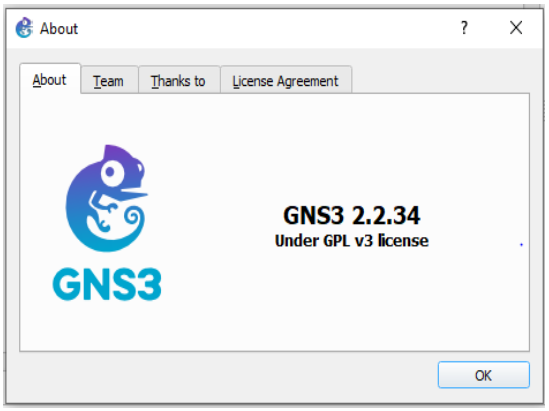
Kabel LAN (*local area network*) atau yang biasa disebut dengan kabel utp adalah kabel yang berguna untuk menghubungkan beberapa komputer/perangkat dalam area yang terbatas contohnya seperti rumah, kantor, laboratorium, perkantoran. Ada beberapa fungsi kabel lan yaitu sebagai berikut:

a. *Kabel LAN* dapat digunakan untuk menghubungkan komputer satu dengan lainnya. Komputer yang saling terhubung dapat melakukan pembagian *file* atau data, tanpa perlu menggunakan media external.
b. Menggunakan LAN untuk menghubungkan dari komputer ke wifi. Performa koneksi menggunakan kabel LAN akan lebih stabil dan cepat dibanding menggunakan *wireless* LAN.
c. Kabel LAN juga digunakan untuk menghubungkan komputer dengan *device* lain. Salah satu contohnya adalah saat menghubungkan komputer dengan printer.

Sesuai dengan kegunaannya kabel LAN dibagi menjadi tiga jenis yaitu kabel *straight through* memiliki urutan kabel yang sama antara ujung satu dengan

ujung lainnya. Kabel *straight* digunakan untuk menghubungkan 2 perangkat yang berbeda, seperti menghubungkan *router* ke *swith/hub*, menghubungkan komputer dengan *router*. Kabel *cross over* memiliki urutan kabel yang berbeda antara *connector* satu dengan *connector* lainnya. Kabel *cross* digunakan untuk menghubungkan dua perangkat yang sama, seperti menghubungkan *router* dengan *router* lainnya, *switch* dengan *switch* lainnya. Kabel *roll over* memiliki urutan kabel yang terbalik antara *connector* satu dengan *connector* lainnya. Kabel *roll* digunakan untuk menghubungkan jaringan dengan *device external*, seperti menghubungkan *switch* dengan printer, menghubungkan *switch* dengan proyektor [16].

2.2.14 GNS3



***Gambar 2. 3*GNS3 2.2.34 [17].**

Gambar 2.3 merupakan aplikasi GNS3 versi 2.2.34. GNS3 (*Graphic Network Simulator*) adalah *software* simulasi jaringan komputer berbasis GUI yang mirip dengan *Cisco Packet Tracer* yangdidirikan pada tahun 2008. Pada GNS3 memungkinkan simulasi jaringan yang kompleks jika dibandingkan dengan jenis simulator lainnya, karena menggunakan *operating system* asli dari perangkat jaringan [17].

2.2.15 WIRESHARK

Gambar 2.4 *Wireshark* [18].

Gambar 2.4 merupakan aplikasi *Wireshark*. *Wireshark* merupakan salah satu *tools* atau aplikasi *capture* paket data berbasis *open-source* untuk melakukan analisis dan pemecah masalah jaringan. Selain itu juga bisa digunakan untuk pengujian *software* karena mampu membaca konten dari tiap paket trafik data. Analisis kerja jaringan melingkupi berbagai hal, dimulai dari proses menangkap paket-paket data atau informasi yang dilalui dalam jaringan sampai memperoleh informasi penting seperti *password email* dan lain sebagainya. Format *file* yang didukung oleh *wireshark* yaitu .cap dan .erf dan adanya alat deskripsi didalamnya juga mampu menampilkan paket-paket terenskripsi dan sejumlah protokol-protokol yang digunakan pada jaringan internet termasuk WEP dan WPA/WPA2 [18].

2.2.16 VLC

***Gambar 2. 5VLC Media Player* [19].**

Gambar 2.5 merupakan aplikasi VLC *media player*. VLC *Media Player* adalah aplikasi pemutar beragam file multimedia baik video maupun audio yang bersifat *open source*. Keunggulan aplikasi VLC *Media Player* yaitu sangat *portable* dan mendukung berbagai ekstensi audio dan video, seperti MPEG-1, MPEG-2, MPEG-4, DivX, mp3, ogg, dll. Aplikasi ini juga bisa digunakan untuk *server streaming* dalam *unicast* atau *multicast* yang bekerja dengan IPv4 atau IPv6 pada jaringan dengan *bandwidth* yang tinggi [19].

2.2.17 Quality of Service

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. QoS digunakan untuk mengukur sekumpulan atribut kinerja yang telah dispesifikasikan dan diasosiasikan dengan suatu servis. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda [20]. Parameter *Quality of Service* terdiri dari:

a. Throughput

Throughput yaitu kecepatan (*rate*) transfer data efektif, yang diukur dalam bps (*bit* per *second*). *Throughput* adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [20].

Tabel 2. 1Kategori *Throughput* [20].

Kategori	***Throughput* (bps)**
Sangat Bagus	100 bps
Bagus	75 bps
Sedang	50 bps
Tidak Direkomendasi	< 25 bbps

$$Throughput = \frac{\text{Paket yang diterima } (bit)}{\text{Waktu pengiriman paket } (second)}$$

b. Delay

Delay (*Latency*) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, *congesti* atau juga waktu proses yang lama [20].

***Tabel 2. 2*Kategori *Delay* [20].**

Kategori	***Delay* (ms)**
Sangat Bagus	< 150 ms
Bagus	150 - 300 ms
Sedang	300 - 450 ms
Tidak Direkomendasi	> 450 ms

$$Delay = \frac{\text{Waktu penerimaan paket} - \text{waktu pengiriman paket}}{\text{Jumlah paket yang diterima}}$$

c. Jitter

Jitter adalah variasi *delay* pengiriman paket yang terjadi pada jaringan IP antara *destination* dan *source*. Faktor yang mempengaruhi besaran nilai *jitter* yaitu variasi beban trafik dan besarnya *congestion* antar paket pada jaringan IP [20].

***Tabel 2. 3*Kategori *Jitter* [20].**

Kategori	***Jitter* (ms)**
Sangat Bagus	0 ms
Bagus	0 – 75 ms
Sedang	75 – 125 ms
Tidak Direkomendasi	125 – 225 ms

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

d. Packet loss

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi karena *collision* dan *congestion* pada jaringan [20].

***Tabel 2. 4*Kategori *Packet Loss* [20].**

Kategori	**Packet Loss (%)**
Sangat Bagus	0 %
Bagus	3 %
Sedang	15 %
Tidak Direkomendasi	25 %

$$Packet\ Loss = \frac{(\text{Paket data dikirim} - \text{paket data diterima})}{\text{Paket data yang dikirim}}$$