BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Pada penelitian Pramawahyudi tahun 2020 [2], berjudul "Evaluasi Kinerja *First Hop Redundancy Protocol* untuk Topologi Star di Routing EIGRP", dalam perancangan jaringan, yang terpenting adalah faktor ketersediaan, mengurangi kegagalan, dan mengatasi beban lalu lintas yang besar. Penelitian ini bertujuan mengimplementasikan dan mengevaluasi sistem *First Hop Redundancy Protocol* (FHRP) pada jaringan topologi star dengan menggunakan *routing* EIGRP. Hasil dari pengujian kinerja rata-rata *delay* menunjukkan selisih antara router *master* dan *backup* pada protokol *Virtual Router Redundancy Protocol* (VRRP) lebih baik yaitu hanya 0,003 detik, sedangkan pada protokol *Gateway Load Balancing Protocol* (GLBP) 0,076 detik dan protokol *Hot Standby Router Protocol* (HSRP) 0,075 detik. Pada pengujian rata-rata *packet loss* protokol GLBP menunjukkan selisih yang cukup besar antara router *master* dan *backup* yaitu 12,07 %, sedangkan pada protokol VRRP 0,07 % dan protokol HSRP 5,06 %. Namun pada hasil pengujian rata-rata *throughtput* protokol HSRP lebih stabil yaitu 0,60 Kbps pada router *master* dan 0,90 Kbps pada router *backup*, sedangkan protokol VRRP paling tidak stabil karena mengalami kenaikan yang signifikan yaitu 0,458 Kbps pada router master dan 1,11 Kbps pada router *backup*.

Pada penelitian Imeldia Ristanti Julia tahun 2020 [3], berjudul "Evaluasi Kinerja *First Hop Redudancy Protocol* (FHRP) pada VRRP, HSRP, dan GLBP dengan *Routing Protocol* BGP dan EIGRP", menjelaskan bahwa dalam membangun infrastruktur jaringan, salah satu hal terpenting adalah bagaimana jaringan dapat menangani kegagalan. Penyedia jaringan, operator jaringan, dan produsen peralatan jaringan lainnya, telah menargetkan ketersediaan jaringan hingga 99,999% (ketersediaan "5 sembilan"), yang berarti bahwa jaringan hanya diperbolehkan untuk mengalami gangguan selama 5 menit dalam satu tahun. Untuk itu diperlukan dua atau lebih gateway yang terkoneksi dalam satu jaringan, karena jika salah satu gateway mati, maka gateway yang lain akan segera menggantikan gateway yang mati tersebut. Penelitian ini akan mengevaluasi performansi *First-*

Hop Redundancy Protocol (FHRP) pada VRRP, HSRP, dan GLBP untuk menentukan perbandingan performansi menggunakan parameter QoS (*throughput*, *jitter*, *packet loss*, dan *downtime*). Metode pengumpulan data menggunakan studi literatur dan metode simulasi dengan 8 tahapan (perumusan masalah, model konseptual, input & output data, pemodelan, simulasi, verifikasi & validasi, eksperimen, dan evaluasi output). Hasil penelitian ini menunjukkan bahwa GLBP memiliki parameter QoS yang lebih baik daripada VRRP dan HSRP.

Pada penelitian Usman Anwar tahun 2019, berjudul "Analisis Kinerja dan Perbandingan Fungsionalitas dari Protokol FHRP", menjelaskan bahwa di era ini, setiap bidang membutuhkan ketersediaan jaringan yang tinggi dengan kemungkinan kehilangan data paling kecil. Oleh karena itu, redundansi harus dilibatkan sebanyak mungkin untuk desain jaringan. Namun ketersediaan jaringan yang tinggi memerlukan biaya manajerial dan operasional yang lebih tinggi. Protokol redundansi secara substansial membantu memecahkan masalah. *First Hop Redundancy Protocols* (FHRP) diimplementasikan untuk mengatasi kehilangan lalu lintas dari sumber ke tujuan dalam komunikasi jaringan. FHRP terdiri dari berbagai jenis protokol. Setiap protokol memiliki tujuan sendiri dan memiliki kelebihan dan kekurangannya sendiri. Protokol ini membantu asosiasi tertentu untuk berhasil mentransmisikan lalu lintas dari sumber ke tujuan tanpa kehilangan banyak paket. FHRP mencakup berbagai jenis protokol tetapi berisi tiga protokol utama. Dalam tulisan ini mengevaluasi tiga protokol khusus FHRP, yaitu *Hot Standby Router Protocol* (HSRP), *Virtual Router Redundancy Protocol* (VRRP), dan *Gateway Load Balancing Protocol* (GLBP). Dalam makalah ini, kami mengevaluasi tiga FHRP dengan menggunakan alat GNS3. Performa dari ketiga protokol FHRP dianalisis dan fungsinya dibandingkan.

Penelitian Arisman Putra Munggaran pada tahun 2018 [5], berjudul "Analisis dan Simulasi Perbandingan QoS di *Routing* Protokol MPLS OSPF dan MPLS IS-IS di Jaringan IPv6 Menggunakan GNS3 untuk Layanan *Video Streaming*" dalam penelitiannya mensimulasikan jaringan IPv6 dengan routing protocol OSPF dan juga IS-IS yang akan ditambahkan teknik MPLS dengan metode xconnect. Setelah itu akan di lakukan analisis QoS untuk layanan *video streaming* pada masing masing *routing* protokol. Simulasi dilakukan menggunakan 1 laptop

yang dibagi lagi menjadi 2 PC dengan menggunakan VMware, simulator yang digunakan adalah GNS3 dan Cisco 7200 sebagai router. Hasil simulasi dan analisis yang didapat menunjukan bahwa *routing* protokol IS-IS yang tidak diterapkan MPLS ataupun dengan MPLS xconnect mendapatkan hasil QoS yang lebih baik dari pada OSPF di jaringan IPv6. Dapat dilihat dari perbedaan throughput hingga 61 Kbps, delay 6 ms, packet loss 3% dan jitter sebesar 3ms. Hal ini disebabkan *routing* protokol OSPF memiliki kompleksitas yang lebih tinggi karena pengenalan *neighbour* OSPF yang lebih rumit di bandingkan IS-IS.

Pada penelitian Bilal Alif Sri tahun 2017 [6], berjudul "Mengurangi *Downtime* Jaringan Komputer Dengan *Hot Standby Router Protocol* Berbasis Cisco di PT Lumbung Riang Communication" meneliti mengenai penerapan *gateway redundancy* menggunakan protokol HSRP yang dilakukan pada dua skenario. Skenario 1 dilakukan pengujian QoS jaringan komputer tanpa HSRP dan dengan HSRP dalam keadaan normal. Skenario 2 dilakukan pengujian QoS jaringan komputer tanpa HSRP dan dengan HSRP ketika terjadi *link failure*. Dari hasil pengukuran dan analisis, pada skenario 1 dapat disimpulkan bahwa diantara jaringan komputer tanpa HSRP dan dengan HSRP, jaringan komputer dengan HSRP memiliki performansi nilai *delay* dan *throughput* yang lebih baik dibandingkan tanpa HSRP. Pada skenario 2 dapat dibuktikan bahwa pada jaringan komputer dengan HSRP memiliki nilai jauh lebih baik semua parameter QoS yang diukur dibandingkan jaringan komputer tanpa HSRP, dikarenakan terdapat fitur *active* dan *standby* router yang selalu siaga ketika terjadi *link failure*.

2.2 DASAR TEORI

2.2.1 Jaringan Komputer

Jaringan adalah seperangkat *device* (biasanya disebut sebagai *nodes*) yang dihubungkan melalui suatu jalur komunikasi. Tujuan dari jaringan komputer yaitu untuk menghubungkan satu *device* dengan *device* lain agar dapat saling bertukar informasi [7]. Jaringan komputer dibedakan menjadi beberapa klasifikasi menurut cakupan jaringannya. Ada perbedaan mendasar yang membedakan jaringan tersebut ke beberapa klasifikasi jaringan komputer diantaranya jaringan LAN, MAN dan WAN.

2.2.1.1 Local Area Network (LAN)

Local Area Network (LAN) adalah jaringan yang menghubungkan perangkat di dalam sebuah gedung atau bangunan yang saling berdekatan dengan bangunan lain nya [8]. Sesuai dengan namanya, LAN berhubungan dengan area *network* yang berukuran relatif kecil. Oleh karena itu, LAN dapat dikembangkan dengan mudah dan mendukung kecepatan transfer data yang cukup tinggi.

2.2.1.2 Metropolitan Area Network (MAN)

Metropolitan Area Network merupakan jaringan yang menggunakan metode sama dengan LAN namun daerah jangkauannya lebih luas. Daerah jangkauan MAN, misalnya satu RW, beberapa kantor yang berada dalam komplek yang sama, satu kota bahkan satu provinsi. MAN merupakan pengembangan dari LAN [7].

2.2.1.3 Wide Area Network (WAN)

Wide Area Network adalah jaringan yang jangkauannya lebih luas daripada MAN. Jangkauan WAN meliputi satu kawasan, satu negara, satu pulau, bahkan satu benua. Metode yang digunakan WAN hampir sama dengan metode yang digunakan pada LAN dan MAN [7].

2.2.2 Redundansi

Desain jaringan redundant memenuhi persyaratan ketersediaan jaringan dengan menduplikasi elemen jaringan. Redundansi adalah sebuah cara pada jaringan yang bertujuan untuk mencegah kegagalan pada *gateway* utamanya dengan mengimplementasikan virtual router yang berarti bahwa kegagalan komponen jaringan apa pun akan menyebabkan kegagalan fungsi seluruh jaringan. Komponen seperti itu bisa berupa router, switch dan jalur antara dua router [9]. Beberapa macam redundansi protokol diantaranya adalah *Gateway Load Balancing Protocol* (GLBP), *Hot Standby Router Protocol* (HSRP) dan *Virtual Router Redundancy Protocol* (VRRP).

2.2.3 *Hot Standby Router Protocol* (HSRP)

HSRP adalah sebuah protokol dari standarisasi CISCO yang membuat router secara otomatis mengambil alih jika terdapat router lain gagal. HSRP memberikan ketersediaan jaringan yang tinggi dengan menyediakan *first-hop redundancy IP address*. HSRP memungkinkan dua buah router interface untuk

bekerja sama dalam membuat satu *virtual* router atau *default gateway* untuk *host* di LAN. Jadi ketika salah satu router yang sudah dikonfigurasi dengan HSRP *down*, maka jalur pada jaringan tersebut akan tetap berjalan, karena IP *gateway* yang dikenal oleh *host* adalah IP *virtual* router. HSRP juga menyediakan *gateway redundancy* dengan *sharing* IP dan alamat MAC anatara *redundant gateways* yang tergabung dalam satu HSRP.[10]

2.2.3.1 Komponen HSRP

Jaringan HSRP memerlukan komponen-komponen untuk mendukung mekanisme kerjanya, diantaranya [9] :

a. *Virtual Router*

Virtual router adalah alamat IP pada perangkat di sisi *user* yang dikonfigurasi sebagai *default gateway*. Router aktif akan memproses semua paket dan frame yang dikirim ke *virtual router*. Apabila salah satu *gateway* router *down*, jaringan akan tetap berjalan karena alamat IP *gateway* yang dikenal *client* adalah alamat *virtual router*.

b. *Address Resolution Protocol* (ARP)

ARP adalah sebuah protokol untuk pemetaan alamat MAC menuju alamat IP yang selanjutnya akan disimpan dalam tabel ARP dari setiap router dalam HSRP grup. Router aktif akan mengirim ulang paket yang dikirim ke MAC *address* pada *virtual router*.

c. *Active Router*

Active router merupakan router aktif yang meneruskan paket yang dikirimkan ke MAC *address* pada *virtual router*.

d. *Standby Router*

Standby router pada HSRP berfungsi untuk memonitor opreasional pada HSRP grup dan bertanggung jawab meneruskan paket jika router aktif tidak beroperasi.

2.2.3.2 Tahapan HSRP

Untuk menjalankan protokol HSRP pada router, terdapat beberapa tahapan yang akan dilalui, berikut adalah tahapan pada protokol HSRP [9] :

a. Initial

Initial adalah tahapan awal dihitung dari saat router masih belum diaktifkan pada *interface* router hingga saat terjadi perubahan saat pengaturan telah dimasukan.

b. Learn

Pada tahapan ini router masih belum menetukan alamat IP virtual dan belum mendapat pesan *hello* dari router aktif. Dalam kondisi ini router masih menunggu pesan dari router aktif.

c. Listen

Pada proses *listen*, router akan mulai menerima paket *hello* dari router lain dimana router lain tersebut juga mengaktifkan protokol HSRP.

d. Speak

Pada tahapan ini, router mulai melakukan pengiriman paket *hello* ke semua router baik aktif maupun *standby*.

e. Standby

Pada tahapan ini salah satu router berada pada posisi *standby*, maka nama dari router tersebut adalah *standby* router. Dalam grup HSRP hanya terdapat satu router yang beroperasi sebagai *standby* router.

f. Active

Ini merupakan tahapan akhir, dimana router akan berposisi sebagai aktif router. Proses yang dilakukan oleh aktif router adalah mengirim paket secara periodik ke router lain yang tergabung dalam satu grup HSRP.

2.2.4 *Gateway Load Balancing Protocol* (GLBP)

GLBP adalalah protokol *redunancy gateway* yang dikembangkan oleh Cisco. GLBP melindungi lalu lintas data dari kegagalan fungsi dari multilayer switch atau router, cara kerjanya hampir sama seperti protokol *Hot Standby Router Protocol* (HSRP) dan *Virtual Router Redundance Protocol* (VRRP). *Gateway Load Balancing Protocol* (GLBP) menyediakan backup router secara otomatis untuk *host* pada jaringan lokalnya. Beberapa router di dalam jaringan lokalnya akan bergabung dalam sebuah grup GLBP sebagai sebuah router secara virtual [11].

GLBP melakukan fungsi yang hampir serupa dengan protokol HSRP dan VRRP namun tidak identik. Protokol HSRP dan VRRP memungkinkan beberapa

router untuk berpartisipasi dalam kelompok router virtual yang dikonfigurasi menggunakan alamat IP virtual. Salah satu anggota kelompok akan dipilih sebagai router aktif yang akan bertanggung jawab untuk meneruskan paket yang dikirim ke alamat IP virtual. Router lain dalam kelompok yang tidak dipilih sebagai router aktif akan menjadi router *standby* sampai router aktif mengalami gangguan. Ketika router aktif masih berfungsi dengan baik maka router *standby* tidak akan melakukan *forwarding* data ini menyebabkan router *standby* seolah – olah menjadi router yang tidak terpakai. Tetapi pada protokol GLBP akan menyediakan *load balancing* melalui beberapa router (*gateway*) menggunakan satu alamat IP *virtual* dan beberapa alamat MAC *virtual*. Setiap *host* akan dikonfigurasi dengan alamat IP *virtual* yang sama, dan semua router pada satu grup router *virtual* berpartisipasi dalam meneruskan paket. Anggota GLBP berkomunikasi satu sama lain melalui pesan hello yang dikirim setiap 3 detik ke alamat multicast ff02::66, port User Datagram Protocol (UDP) 3222 dan memiliki hold time sebesar 10 detik untuk menyatakan router dalam kondisi down [10].

2.2.4.1 Mekanisme Kerja GLBP

a. Active Virtual Gateway

GLBP memungkinkan untuk mendapatkan alamat MAC *virtual* sebanyak 4 alamat per grup. AVG bertanggung jawab untuk menetapkan alamat MAC *virtual* ke setiap anggota grup. Anggota grup lainnya meminta alamat MAC virtual melalui pesan *hello* kepada AVG. *Interface* yang diberikan alamat MAC *virtual* oleh AVG disebut dengan *active virtual forwarder* (AVF). AVF yang diberi alamat MAC virtual pertama kali oleh AVG dikenal sebagai *virtual forwarder* utama. AFV utama inilah yang nantinya akan mengambil alih tugas dari AVG pada saat AVG mengalami gangguan. sedangkan anggota grup GLBP lainnya yang mempelajari alamat MAC virtual dari pesan *hello* disebut sebagai *forwarder virtual sekunder*. AFV juga berfungsi untuk meneruskan paket dari wilayah jaringan lokal ke wilayah jaringan luar [9].

b. Virtual Gateway Redundancy

Menjalankan *Virtual Gateway Redundancy* pada GLBP sama dengan HSRP. Gateway yang berwenang untuk memutuskan adalah AVG sedangkan gateway lainnya sebagai *standby virtual gareway* dan *gateway* yabg tersisa

ditempatkan di tempat yang mudah diperhatikan. Jika terjadi kerusakan pada AVG, maka *standby virtual gateway* akan menerima tanggung jawab sebagai *virtual IP address. Standby virtual gateway* yang baru akan ditempatkan di tempat yang mudah diperhatikan.[9]

c. Virtual Forwarder Redundancy

Virtual Forwarder Redundancy sama seperti Virtual Gateway Redundancy dengan suatu AVF. Apabila AVF mengalami gangguan, maka *Secondary Virtual Forwarder* (SVF) akan menerima status dan bertanggungjawab pada *Virtual MAC Address.* AVF yang baru akan menjadi *primary virtual forwarder* untuk sebuah nomor *forwarder* yang berbeda.[9]

2.2.5 IPv6

IPv6 adalah perkembangan dari IPv4 yang bertujuan untuk mem-*backup* kekurangan kebutuhan IP. Pada IPv4 menggunakan sistem pengalamatan 32 bit, sedangkan pada IPv6 sebesar 128 bit. Besaran bit ini mengartikan banyaknya alamat IP yang dapat dihasilkan, misal pada 32 bit maka jumlah IP yang ada sebanyak 2 pangkat 32 dan 128 bit maka jumlahnya adalah 2 pangkat 128. [12]

Tabel 2.1 Perbedaan IPv4 dan IPv6

	IPv4	IPv6
Dipublish	1981	1999
Ukuran Alamat	32 bit	128 bit
Format Alamat	Decimal, 192.168.255.1	Hexadecimal, 2F1D::ABCD
Notasi Prefix	192.168.0.0/24	2F1D::ABCD/48
Jumlah Alamat	2^{32} = 4.294.967.296	2^{128} = 3,402823669 $\times 10^{38}$

IPv6 Menyediakan 3 jenis pengalamatan meliputi *Unicast*, *Anycast* dan *Multicast*. *Unicast* menunjukan pada alamat untuk komunikasi satu lawan satu, atau antar *host*. *Unicast* sendiri dibagi lagi menjadi 3 bagian, yaitu *link local, site local* dan alamat global. *Link local* adalah suatu alamat yang diperuntukan dalam satu *link* yaitu jaringan *local* dalam satu *level*. *Site local* merupakan alamat yang dipakai terbatas hanya dalam satu *site* penggunanya terbatas dan juga tidak dapat mengirimkan alamat diluar *site*, ini hampir sama halnya dengan alamat *private*.

Alamat global adalah alamat yang dipakai untuk *Internet Service Provider* (ISP). *Anycast* merupakan alamat yang menunjukan beberapa *interface*, umumnya berbeda node namun berdekatan. Contohnya paket yang dikirimkan ke alamat ini akan diteruskan ke salah satu alamat *host* namun yang terdekat dengan router. Sedangkan *multicast* adalah alamat yang menunjukan berbeda node. Paket yang dikirimkan ke alamat ini akan ke semua *interface* yang ditunjukan ke alamat awal sama halnya dengan alamat broadcast.[13]

2.2.6 *Routing*

Routing adalah suatu aturan yang digunakan untuk mencari route pengiriman paket dari satu jaringan ke jaringan lain. Router akan membuat keputusan berdasarkan alamat IP yang dituju oleh paket. Semua router menggunakan alamat IP tujuan untuk mengirim paket. Agar keputusan *routing* tersebut benar, router harus belajar bagaimana mencapai tujuan. Ketika router menggunakan *routing* dinamis, informasi ini dipelajari dari router lain. Ketika menggunakan *routing* statis, seorang admin jaringan mengkonfigurasi informasi tentang jaringan yang akan dituju secara manual. [14]

Jika *routing* yang digunakan adalah statis, konfigurasi akan dilakukan secara manual, admin jaringan harus memasukan atau menghapus rute statis jika terjadi perubahan topologi. Pada jaringan skala besar, jika tetap menggunakan *routing* statis, maka akan membuang waktu admin jaringan untuk melakukan perbaruan tabel *routing*. Karena itu *routing* statis hanya mungkin dilakukan untuk jaringan skala kecil. Sedangkan *routing* dinamis bisa diterapkan di jaringan skala besar dan membutuhkan kemampuan lebih dari admin jaringan.

Routing protokol secara umum dibagi menjadi dua yaitu *Distance-Vector* dan *Link State*. *Distance-Vector* menggunakan algoritma Bellman-Ford, yang bekerja berdasarkan perhitungan jalur terpendek dari satu node ke node yang lain dengan mempertimbangkan bobot tepi negatif. Data kemudian diteruskan menggunakan jalur terbaik yang dipilih dari tabel *routing*. *Distance-Vector* diklasifikasikan dalam RIP (versi 1 dan versi 2) dan EIGRP. *Link State Routing Protocol* menghitung jalur terbaik dari sumber ke tujuan menggunakan algoritma Djikstra, kemudian menyajikan informasi ini ke semua router yang bersebelahan. *Link State* diklasifikasikan ke dalam OSPF dan ISIS. [15]

2.2.6.1 Open Shortest Path First (OSPF)

OSPF adalah routing protokol yang merupakan peningkatan RIP, dengan konvergensi yang lebih cepat dan parameter yang lebih dapat dikonfigurasi. OSPF mengirimkan paket *hello*, menghubungkan permintaan negara, pembaruan dan deskripsi basis data, serta menerapkan algoritma Djikstra untuk menentukan jalur terpendek ke tujuan. Pembaruan terbatas ketika ada perubahan, meskipun tabel *Link State Advertising* (LSA) di-*refresh* setiap 30 menit. OSPF mengimplementasikan *routing* hirarkis, dengan membatasi jaringan yang berbeda ke beberapa area. [15]

Penggunaan konsep hirarki pada OSPF membuat protokol akan membagi area jaringan ke dalam beberapa dimensi area. Ini akan sangat berpengaruh dalam pengiriman data karena dengan hirarki ini akan lebih memudahkan dalam keteraturan pengiriman data. Data yang akan dikirim tidak akan tersebar kesana-kemari karena sudah tersegmentasi. Penggunaan *bandwidth* akan lebih efisien karena sudah ada keteraturan dalam distribusi pe-*routing*-an. OSPF terbagi menjadi dua yaitu OSFP versi 2 dan OSPF versi 3. Versi 2 mendukung implementasi IPv4 sedangkan versi 3 mendukung IPV6.

2.2.7 *Video Streaming*

Video merupakan suatu media yang sangat penting untuk komunikasi dan hiburan pada masa kini. Pertama kali, *video* diolah dan ditransmisikan dengan bentuk analog. Perkembangan di bidang teknologi informasi telah membantu terbentuknya *video* digital. Salah satu penerapan *video* digital yang digunakan dalam transmisi data adalah video streaming.

Video streaming adalah teknologi pengiriman data, *video* atau *audio* dalam bentuk yang telah dikompresi melalui jaringan internet yang ditampilkan oleh suatu *player* secara *realtime*. Pengguna memerlukan *player* yang merupakan aplikasi khusus untuk melakukan dekompresi dan mengirimkan data berupa *video* ke tampilan layar monitor dan data berupa suara ke speaker. Sebuah *player* dapat berupa suatu bagian dari *browser* atau sebuah perangkat lunak. Inti dari *streaming* adalah membagi data dan *encoding*, kemudian mengirimkannya melalui jaringan dan pada saat data sampai pada pengguna maka akan dilakukan *decoding* serta pembacaan data.[16] Ciri-ciri aplikasi streaming yaitu distribusi *audio*, *video* dan

multimedia pada jaringan secara *realtime* atau *on demand*, transfer media data digital dari server dan diterima oleh pengguna sebagai *realtime stream* simultan sehingga pengguna tidak perlu menunggu keseluruhan data di unduh karena server mengirimkan data yang diperlukan setiap selang waktu tertentu. Hal ini memungkinkan pengguna untuk menjalankan *file content* seketika dengan periode *buffer* pendek.

Ada beberapa tipe *video streaming* antara lain *webcast*, dimana tayangan yang ditampilkan merupakan siaran langsung (*live*) dan *Video on Demand* (VOD), di mana tayangan yang akan ditampilkan sudah terlebih dahulu disimpan dalam *server*. Faktor-faktor yang mempengaruhi distribusi *video streaming* melalui jaringan antara lain: besarnya *bandwidth*, waktu tunda (*delay*), *lost packet*, dan juga teknik mendistribusikan *video* tersebut ke beberapa tujuan secara merata dan efisien.[16]

2.2.7.1 Cara Streaming

Ada tiga cara umum yang biasa digunakan dalam menerima *stream* data yaitu :

a. Download

Pada penerimaan *stream* data dengan cara *download*, akses *video* dilakukan dengan cara melakukan *download* terlebih dahulu suatu file multimedia dari server. Penggunaan cara ini mengharuskan keseluruhan suatu file multimedia harus diterima secara lengkap pada pengguna. File multimedia yang sudah diterima kemudian disimpan pada tempat penyimpanan yang ada di komputer. Pengguna baru dapat mengakses *video* tersebut setelah berhasil menerima file multimedia tersebut secara lengkap. Keuntungan dari penggunaan cara *download* ini adalah akses yang lebih cepat ke salah satu bagian dari *file* tersebut. Sedangkan kekurangannya adalah pengguna yang ingin mengakses video tersebut harus menunggu terlebih dahulu sampai keseluruhan *file* multimedia tersebut diterima secara lengkap.

b. Streaming

Pada penerimaan video secara *streaming*, pengguna dapat melihat suatu *file* multimedia hampir bersamaan ketika *file* tersebut mulai diterima. Penggunaan cara ini mengharuskan pengiriman suatu *file* multimedia ke pengguna secara konstan.

Hal ini bertujuan agar pengguna dapat menyaksikan video yang diterima secara langsung tanpa ada bagian yang hilang. Keuntungan dari cara ini adalah pengguna tidak perlu menunggu hingga suatu *file* multimedia dikirimkan secara lengkap. Dengan demikian, penggunaan cara ini memungkinkan sebuah *server* untuk melakukan pengiriman siaran secara langsung kepada pengguna.

c. Progressive Downloading

Progressive downloading adalah suatu metode *hybrid* yang merupakan hasil penggabungan antara metode *download* dan metode *streaming*, dimana video yang sedang diakses dapat diterima dengan cara *download* sehingga *player* yang ada pada pengguna sudah dapat mulai menampilkan video tersebut sejak sebagian dari *file* tersebut diterima walaupun *file* tersebut belum diterima secara lengkap.

2.2.7.2 Komponen *Streaming*

Dalam menjalankan video streaming, terdapat beberapa komponen diantaranya :

a. Input

Sumber dari video yang akan di-*streaming*. Sumber tersebut dapat berupa *file* video, DVD, MPEG, dan lain-lain.

b. Encoder

Bagian dari aplikasi *server* yang bertugas untuk mengubah video sumber menjadi sebuah format yang sesuai dengan transmisi *streaming*, dimana format ini umumnya memiliki tingkat kompresi tinggi sehingga dapat ditransmisikan dengan baik pada suatu media jaringan.

c. Server

File hasil *encoding* kemudian didistribusikan oleh *server* kepada pengguna. Pada aplikasi yang digunakan, *encoder* dan *server* berada pada satu aplikasi yang sama yang terintegrasi satu sama lain.

d. Player / Output

Player berfungsi untuk melakukan *decoding* terhadap *file* hasil *streaming* dan menampilkannya pada pengguna.

2.2.8 *Quality of Service* (QOS)

Quality of Service (QoS) merupakan pengukuran mengenai seberapa baik kualitas dan merupakan mekanisme jaringan yang memungkinkan aplikasi –

aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan seperti pada pada aplikasi jaringan, *host* atau *router* untuk memiliki tingkatan jaminan bahwa elemen jaringan tersebut dapat memenuhi kebutuhan suatu layanan. Beberapa parameter uji untuk *Quality of Service* (QOS) antara lain [17]:

2.2.8.1 Delay

Delay merupakan waktu yang dibutuhkan oleh suatu paket data untuk menempuh jarak saat dikirim hingga sampai ke tujuan dan melewati antrian pengiriman yang padat. Parameter standarisasi *delay* menurut *Telecomunication and Internet Protocol Harmonization Over Network* (TIPHON) dapat dilihat pada tabel 2.1

Rumus untuk menghitung *delay* :

$$Delay = \frac{\text{Waktu penerimaan paket} - \text{waktu pengiriman paket}}{\text{jumlah paket yang diterima}} \quad (2.1)\ [17]$$

Tabel 2.2 Standarisasi Delay

Kategori *Delay*	***Delay***
Sangat bagus	<150 ms
Bagus	150 ms s/d 300 ms
Sedang	300 ms s/d 450 ms
Buruk	>450 ms

2.2.8.2 Packet Loss

Packet loss merupakan parameter yang menunjukan besarnya nilai paket yang hilang akibat adanya penurunan sinyal pada jaringan, paket yang rusak serta kesalahan yang terjadi pada *hardware*. Saat terjadi *packet loss* maka penerima akan meminta retransmisi sehingga dapat mengurangi nilai efisiensi pada jaringan. Parameter standarisasi untuk *packet loss* menurut *Telecomunication and Internet Protocol Harmonization Over Network* (TIPHON) dapat dilihat pada tabel 2.2 [17]

Tabel 2.3 *Standarisasi Packet Loss*

Kategori *Packet loss*	***Packet loss***
Sangat bagus	0%
Bagus	3%
Sedang	15%

Buruk	25%

2.2.8.3 Throughput

Throughput adalah bandwidth aktual yang terukur pada suatu ukuran waktu tertentu dalam suatu hari menggunakan rute *internet* yang spesifik ketika sedang melakukan *download* suatu file. *Throughput* menunjukkan perbandingan antara paket data yang berhasil sampai tujuan dengan waktu pengamatan. Satuan yang dipakai untuk analisis *throughput* ini adalah bps (*bit per second*). [20]

Rumus untuk menghitung *Throughtput:*

$$\text{Throughput(bps)} = \frac{\text{Paket data yang diterima (bit)}}{\text{Waktu pengiriman paket (second)}} \text{ (2.2) [17]}$$

2.2.8.4 Jitter

Jitter merupakan variasi *delay* yang terjadi akibat adanya selisih waktu atau *interval* antar kedatangan paket di penerima. Parameter standarisasi untuk *packet loss* menurut *Telecomunication and Internet Protocol Harmonization Over Network* (TIPHON) dapat dilihat pada tabel 2.4 [17]

Rumus untuk menghitung *Jitter:*

$$Jitter = \frac{\text{variasi delay}}{\text{jumlah pengukuran}} \quad \textit{(2.3)} \text{ [17]}$$

Tabel 2.4 Standarisasi *Jitter*

Variasi Waktu Tunda (ms)	**Kualitas**
0-20 ms	Baik
20 – 50 ms	Cukup, masih dapat diterima
>50 ms	Tidak dapat diterima