BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian yang dilakukan oleh Kukuh Nugroho, Muhamad Syamsul Fallah pada tahun 2018 yang berjudul ”*Implementasi Load balancing Menggunakan Teknologi Etherchannel pada Jaringan LAN”* meneliti tentang peningkatan jumlah pengguna yang menyebabkan menurunnya kualitas jaringan ketika menggunakan *bandwidth* yang sama. Seperti halnya pada jaringan kampus yang menghubungkan jaringan antar Gedung menggunakan perangkat *switch*. Penurunan performa jaringan dapat datasi dengan menggunakan *Load balancing* teknologi *Etherchannel* dengan protokolnya yaitu protokol PAgP dan LACP. Penelitian ini melakukan uji coba menggunakan konsep *client-server*, yang mana *server* akan bekerja sebagai tempat untuk mengimplementasikan aplikasi FTP untuk layanan pertukaran data dan untuk implementasi layanan video *streaming dan Client* akan mengakses data pada *server*. Dari hasil penelitian tersebut dihasilkan nilai *delay* dengan protokol PAgP memiliki nilai sebesar 42% lebih baik jika dilakukan perbandingan dengan protokol LACP, pengukuran *throughput* juga menunjukan nilai lebih baik 10% dibandingkan dengan protokol LACP [5].

Muhammad Zulfi Rahmanzi, Iskandar Fitri, Andri Aningsih pada tahun 2021 dengan penelitiannya yang berjudul ”*Kinerja Load balancing pada Teknologi Etherchannel Menggunakan Metode VLAN Trunking Protocol (VTP)*” membahas mengenai bagaimana kinerja yang ada pada *Load balancing* teknologi *Etherchannel* metode *Virtual Trunking Protocol* (VTP). Dimana dalam topologi jaringan yang sudah dibuat terdapat konfigurasi *Virtual local area network* dan teknologi *etherchannel* dimana kedua konfigurasi tersebut dilihat sebagai implementasi dan pengaruhnya ketika sebuah metode VTP diterapkan untuk menganalisis kinerja jaringan VTP dapat berjalan dengan efisien atau tidak dengan protokol LACP dan PagP. Penelitian ini melihat hasil analisis QoS selama 1 jam dan memiliki beberapa skenario yaitu ketika jalur terhubung dan beberapa jalur diputus. Saat kondisi semua terhubung memiliki nilai rata-rata *throughput* 1,8 Mb/s dan *packet loss* 8,1%. Pengujian kedua kondisi CORE_SW2 dimatikan,

mendapat rata-rata *throughput* 1,8Mb/s dan *packet loss* 8,2%. Saat pengujian ketiga kondisi jalur Po1 diputus, koneksi dialikan ke 2 jalur. Po5 mendapatkan rata-rata *throughput* 15Mb/s dan *packet loss* 23,15%, Po2 mendapatkan *throughput* 1,8 Mb/s dan *packet loss* 8,7%. Maka pengaruh teknologi *Etherchannel* saat kondisi pertama dan kedua tergolong baik, sedangkan saat kondisi ketiga *throughput* tergolong luar biasa, tetapi *packet loss* yang dihasilkan berkondisi sedang. [6].

Sedangkan Alfin Syaifudin, Moh. Iwan Wahyuddin, dan Sari Ningsih pada tahun 2020 dengan penelitiannya yang berjudul "Perancangan Redudancy *Link* dan *Load balancing* Menggunakan Metode *Etherchannel* LACP dengan InterVLAN *Routing*" membahas mengenai koneksi jaringan LAN yang terganggu akibat masalah muncul ketika jaringan digunakan. Permasalahan tersebut dapat ditangani dengan menggunakan salah satu teknologi pada jaringan LAN yaitu teknologi *Etherchannel*. Penelitian ini menerapkan teknologi *Etherchannel* tipe LACP dan *Load.* Dari penerapan teknologi tersebut, masalah yang muncul akibat jaringan LAN dapat teratasi dan mengakibatkan peningkatan ketersediaan jaringan dan kecilnya resiko *overload* dengan performa jaringan yang baik. Penelitian ini menghasilkan beberapa kesimpulan diantaranya pada kondisi 30, 40 dan 50 PC rata-rata nilai *packet loss* kurang dari 1% dan *delay* tidak lebih dari 150 ms [1].

2.2 DASAR TEORI

2.2.1 Jaringan Komputer

Pada dasarnya jaringan komputer berasal dari kata jaringan dan komputer. Jaringan merupakan suatu keterkaitan komunikasi yang terhubung satu dengan lainnya dan dapat saling berkomunikasi (*interconnected*), sedangkan komputer dapat dikatakan sebagai perangkat yang digunakan sebagai alat komunikasi. Dari gabungan kedua kata tersebut disimpulkan bahwa jaringan komputer adalah kumpulan beberapa perangkat komunikasi yang saling berhubungan (komputer, dsb)[7].

Jaringan dapat dibedakan menjadi jaringan *privat* maupun *public*. Dalam penggunaan jaringan privat, umumnya membutuhkan akses user guna yang berupa kata sandi yang di-*input*-kan secara manual oleh seorang administrator atau langsung diperoleh seorang pengguna. Sedangkan pada penggunaan jaringan publik contohnya internet, tidak akan membatasi suatu akses.

Jaringan komputer memiliki beberapa jenis, diantaranya LAN, MAN, WAN. Dari beberapa jenis jaringan komputer tersebut berikut penjelasan terkait macam-macam jaringan komputer :

1. LAN (*Local Area Network*), merupakan jaringan yang memiliki ruang lingkup terbatas seperti Gedung, kampus, kantor, pabrik dan lainnya. LAN ini banyak sekali digunakan untuk jaringan yang berada di daerah perkantoran, bisnis, dan sebagainya yang memiliki skala kecil. LAN dapat dibangun dengan minimal 2 komputer saling terhubung, walaupun komputer dengan spesifikasi yang rendah sekalipun.
2. MAN (Metropolitan Area *Network*), jaringan ini merupakan jaringan komputer yang memiliki jarak komunikasi yang cukup jauh. Biasanya tipe ini sering digunakan untuk membangun sebuah jaringan komputer antar Gedung, jaringan dalam suatu kota, atau antar kota yang masih dalam area jangkauannya. Pemilihan jaringan ini biasanya digunakan oleh perusahan besar seperti perbankan, dan kantor besar sejenisnya.
3. WAN (*Wide* Area *Network*), jaringan tipe ini termasuk kedalam tipe jaringan yang terbesar, karena mencangkup jarak jangkau komunikasi yang sangat

jauh, seperti antar negara bahkan benua tanpa suatu Batasan geografis seperti jaringan yang lain [8]

2.2.2 *Layer* OSI (*Open System Interconnected)*

Layer OSI dikenalkan pertama kali pada tahun 1977 oleh ISO, atau dikenal dengan *International Organization for Standarization*. OSI Model memiliki tujuh *layer* dan sistemnya biasa digunakan Model OSI terdiri dari tujuh lapisan dan sistem ini terkenal karena set lapisan yang dibagi secara komprehensif. Berikut *layer-layer* yang terdapat pada OSI *layer*.

2.2.2.1 *Physical layer*

Lapisan fisik adalah listrik dan representasi mekanis dari sistem OSI karena menyampaikan aliran bit dalam bentuk impuls listrik atau cahaya atau sinyal radio. Lapisan ini meliputi kabel, radio frekuensi *link, layout* pin. Jika ada masalah fisik di dalam jaringan, lapisan ini adalah tempat untuk memeriksanya yang harus dipastikan pada *layer* ini bahwa semua kabel terhubung dan steker listrik utuh atau tidak. Lapisan fisik ini menyediakan perangkat keras untukmengirim dan menerima data pada operator, termasuk menentukan kabel, kartu, dan aspek fisik lainnya. Beberapa contoh komponen lapisan fisik ini adalah fast *ethernet*, RS232, ATM dan lainnya [9].

2.2.2.2 *Data link Layer*

Layer ini mengatur pengiriman data dari *interface* yang berbeda. Data *Link layer* memiliki beberapa fungsi diantaranya :

1. Arbitration, pemilihan media fisik

Penentuan waktu pengiriman data yang tepat apabila suatu media sudah terpakai, hal ini perlu melakukan suatu deteksi sinyal pembawa. Pada ethernet menggunakan metode *Carrier Sense Multiple Access / Collision Detection* (CSMA/CD).

Pada jaringan yang dapat melakukan akses secara bersamaan simultan. Maka apabila suatu host mengirimkan data ke host yang lain, maka host selain pengirim dan penerima akan melakukan deteksi jalur, dan apabila jalur sedang dipakai maka host selain pengirim dan penerima akan menunggu terlebih dahulu. Hal tersebut dapat mencegah terjadinya *collision.*

2. *Addressing*

Pengalamatan yang dilakukan pada *layer* data *link* bersifat fisik, yaitu menggunakan Media Access Control (MAC). MAC ditanamkan pada interface suatu perangkat jaringan. MAC berukuran 48 bit dengan format 12 heksadesimal.

3. *Error Detection*

Teknik yang digunakan adalah *Frame Check Sequence* (FCS) dan *Cyclic Redundancy Check* (CRC) [18].

2.2.2.3 *Network Layer*

Fungsi utama dari *layer network* diantaranya adalah sebagai berikut :

1. Fungsi *Router*, sebuah *router* merupakan sebuah perangkat jarigan yang bekerja dengan mentransfer data dalam bentuk paket-paket dan bisa mengkoneksikan dua atau lebih jaringan yang berbeda secara bersamaan.
2. *Packet forwarding*, adalah proses transfer data paket dari pengirim (*host*)
3. Teknologi *switch*, pada fungsi ini mengizinkan transmisi data dari node ke node dengan menggunakan jalur *logic* dimana mungkin juga bisa digunakan sebagai jalur virtual.

2.2.2.4 *Transport Layer*

Lapisan ini memastikan lengkap dan transparannya data transfer dari dan ke tujuan end device. Koordinasi data transfer ini merupakan tujuan utama dari *layer transport* yang berkaitan dengan dimanakah data dikirimkan, kecepatan data yang dikirimkan dan berapa banyak data yang ditransmisikan. Salah satu lapisan *transport* yang paling banyak digunakan adalah TCP (Transmission Control *Protocol*). TCP terletak di bagian atas IP lapisan yang akan mengirimkan kembali paket data ketika di dalam perjalanan menuju klien sehingga ketika didalam sebuah jaringan yang padat akan berdampak pada kongestinya yang semakin meningkat. Sedangkan *transport layer* lainnya yaitu UDP (*User Datagram Protocol*) yang merupakan prototokol dengan kecepatan pengiriman data tanpa memperhatikan adanya *control* konjesti dan koreksi kesalahan di dalam suatu jaringan dengan menggunakan bandwidthnya secara penuh. Fungsi utama lapisan ini adalah *end-to-end error recovery* dan *flow control.*

2.2.2.5 *Session Layer*

Session layer bekerja ketika perlu dilakukan untuk membuat suatu *session* dimana ketika dua perangkat fisik seperti komputer atau servr membutuhkan untuk komunikasi satu dengan lainnya. Fungsi utama dari sesi ini yaitu :

1. Pengaturan, inisiasi sebuah sesi untuk mengijinkan berkomunikasi
2. Koordinasi, mengizinkan transfer data informasi dan menentukan waktu respon
3. Terminasi, untuk mengakhiri sesi

Dalam kata lain, *layer* ini bekerja dengan mengkoordinasikan koneksi antara dua perangkat untuk saling berkomunikasi, termasuk prosedur pengaturan, membangun informasi yang aman, manajemen koneksi, koordinasi komunikasi dan pertukaran data informasi serta pemutusan sebuah aplikasi dalam kedua device dalam akhir sesi

2.2.2.6 *Presentation Layer*

Layer ini berfungsi sebagai penyaji data ke jaringan, hal tersebut juga bisa disebut sebagai lapisan sintaks. Hal ini memungkinkan transfer data dari *layout* aplikasi ke *layout network* atau serupa dari jaringan *layout* ke aplikasi *layout*. Dengan kata lain, laisan ini berhubungan dengan data yang dikecualikan dari representasi data pada aplikasi. Contohnya adalah ekripsi data atau dekripsi data untuk mengamankan transmisi data.

2.2.2.7 *Application Layer*

Layer aplikasi adalah alyer yang berada paling atas dari *layer* osi yang ada. *Layer* ini dikatakan sebagai *layer* yang paling dekat dengan *end user* karena *layer* ini merupakan *layer* yang lasung berinteraksi dengan pengguna jaringan dan dapat dilihat oleh pengguna. *Layer* aplikasi ini dapat membantu pengguna untuk menerima informasi langsung and data di tampilkan juga. Contohnya adalah seperti *goolge chrome, firefox, safari*. Fungsi utama dari *layer* ini adalah [9]:

1. Mengidentifikasi komunikasi lawan
2. Mendukung aplikasi
3. Mengidentifikasi *quality of service*
4. Mendukung proses-proses pengguna

5. Mengidentifikasi segala kendala dalam data *syntax*

2.2.3 *Virtual Local Area Network*

Virtual local area network (VLAN) merupakan Teknik yang digunakan sebagai pemecah *Local Area Network* (LAN) menjadi beberapa jaringan lagi atau bisa dikatakan sebagai pemecah wilayah *broadcast* dalam sebuah perangkat yang bernama *switch*. Ketika sebuah komputer mengirimkan data secara *broadcast*, maka data tersebut akan diteruskan ke semua *port* selain *port* yang digunakan oleh komputer pengirim untuk mengirimkan data *broadcast* sebelumnya [4]. *Switch* dapat dihubungkan dengan *router* untuk menghubungkan sebuah jaringanVLAN yang telah ditentukan.

Pada jenis *switch* ini tetap dengan fungsi yang sama namun banyak fitur-fitur tambahan yang dapat meningkatkan kualitas dari jaringan tersebut, contoh fitur yang paling sering digunakan adalah kemampuan *switch* dalam membuat VLAN dan *control traffic* jaringan, *switch* ini juga dapat melakukan proses *routing*, berbeda halnya dengan *switch unmanageable* yang hanya bekerja di *layer* 2 yaitu *layer data link*, namun pada *switch manageable* dapat dilakukan proses *routing* ataupun menghubungkan alamat IP yang berbeda, dalam hal ini *switch* bekerja di *layer* 3.

Selain dengan kemampuan untuk membuat VLAN dan *control traffic* jaringan, *switch* ini juga dapat meningkatkan keamanan dengan menggunakan kemampuan *switch port security* yang berfungsi untuk menangani hak akses kejaringan tersebut berdasarkan *port – port* yang dimiliki oleh *switch* tersebut [19].

2.2.4 *Inter-vlan*

Inter-VLAN adalah *routing* yang menghubungkan antar VLAN yang berbeda yang di konfigurasi didalam *router*. *Router*-on-stick biasanya disebut sebagai default gateway dari tiap VLAN yang diatur dalam *router* untuk dipasang kedalam *sub interface* dimana *router* yang menerapkan kosep *inter-vlan* iniakan meneruskan trafik jaringan dari suatu VLAN ke VLAN lainnya [3].

Inter-VLAN routing melakukan *forwarding traffic* dari VLAN yang sat uke VLAN lainnya dengan menggunakan *router*, pada jaringan ini sistem routing dapat terpusat dan hanya membutuhkan satu *router* dan satu *port* interface untuk pembagian ip address yang akan dibuat dalam bentuk virtual yang kemudian akan di trunk menuju VLAN lainnya yang ada di *switch* pada Gedung-gedung yang berbeda. Default inter-VLAN routing akan banyak membutuhkan *port* untuk tiap network yang berbeda namun dapat menggunakan trunk untuk memanfaatkan banyak ip yang berbeda melewati satu jalur yang sama [19].

2.2.5 ACL (*Access Control List*)

ACL digunakan untuk mengamankan dan mengontrol lalu lintas antara masuk dan keluar dari jaringan. Dalam implementasi modern, file pusat server dan layanan biasanya ditempatkan di tempatnya masing-masing yang terisolasi VLAN, mengamankannya dari kemungkinan serangan jaringan saat mengontrol akses ke pengguna. Seorang administrator dapat menonaktifkan ICMP dan protokol lain yang digunakan untuk mendeteksi *broadcast host* untuk menghindari kemungkinan deteksi oleh *host* penyerang yang berada di VLAN yang berbeda. Setelah ACL dikonfigurasi di *router*, *router* berubah fungsi menjadi firewall dan memeriksa setiap pernyataan berurutan sebelum meneruskan trafik ke tujuannya. Dengan menggunakan daftar akses ini, *router* memproses setiap ACL dari atas ke bawah dalam satu waktu. ACL dapat dilakukan untuk menyarik trafik antara VLAN atau antara *host* dari VLAN serta dapat menggunakan ACL sebagai standar untuk membatasi akses telnet dari jarak jauh [10].

2.2.6 Pengalamatan *IP Address*

IP Address adalah suatu alamat yang diberikan ke peralatan jaringan komputer untuk dapat diidentifikasi oleh komputer yang lain dengan demikian masing masing komputer dapat melakukan proses tukar menukar data informasi, mengakses internet, atau mengakses ke suatu jaringan komputer dengan menggunakan protokol TCP/IP. *IP Address* biasanya digunakan sebagai pengidentifikasi sebuah *interface* suatu jaringan *host* dari satu komputer dan

terdiri dari bilangan biner 32 bit yang dibagi lagi menjadi 4 bagian. Masing-masing bagian terdiri dari 8 bit, dimana memiliki nilai desimal dari 0 sampai 255. Tiap 8 bit ini disebut sebagai oktet [1].

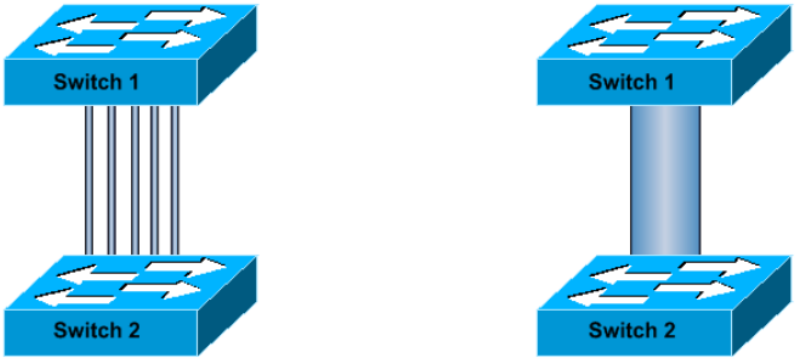
2.2.7 OSPF *Routing Protocol*

Open Shortest Path First adalah sebuah protokol *routing link* state yang biasanya digunakan untuk menghubungkan dari *router* ke *router* yang lain yang masih dalam satu *autonomous system (AS).* Protokol ini termasuk dalam kategori *Interior Gateway Protocol* (IGP). OSPF ini bekerja hanya dalam jaringan internal suatu organisasi atau sebuah perusahaan. Konsep pe*rute*an OSPF ini memiliki sistem penyebaran indormasi data yang teratur dan tersegmentasi, sehingga penyebarannya teratur. Sehingga *bandwidth* yang dipakai pun menjadi lebih efisien, lebih cepat untuk mencapai konvergensi, serta lebih akurat untuk menentukan *rute-rute* yang paling baik untuk mencapai sebuah lokasi informasi yang akan dituju [11].

2.2.8 *Etherchannel* (*Port-Channel*)

Switch menggunakan sebuah teknologi *link* aggregation *port* yang dinamakan *etherchannel* atau *port-channel*. Teknologi ini mengizinkan multi interface *ethernet* menjadi satu jalur *logic* interface *ethernet* yang ditunjukan pada gambar 2.1, jalur *logic* tersebut digunakan untuk menyediakan kecepatan pengiriman antar jalur yang ada pada *switch*, server, maupun *router* juga memberikan toleransi kesalahan untuk perangkat tersebut [12].

Etherchannel digunakan di antara *switch* dan server dan dapat terbentuk dari dua sampai delapan buah interface yang aktif dan juga dapat digunakan di jaringan backbone. Terkadang digunakan untuk menghubungkan klien *end device*[12].



Gambar 2. 1 Tampilan Fisik dan Logik dari Teknologi *Port-Channel* [2]

berikut beberapa fungsi yang dijalankan oleh *port-channel* :

1. Dapat digunakan untuk meningkatkan *aggregate bandwidth* di dalam jalur dengan mendistribusikan *'band'* antara jalur yang aktif di *channel* tersebut
2. Menerapkan keseimbangan dalam memuat data melewati beberapa jalur dan memelihara *bandwidth* untuk mencapai penggunaan yang optimal
3. Menyediakan toleransi kesalahan yang tinggi, jika satu jalur mati trafik akan di pindahkan secara langsung ke jalur lainnya dalam satu *channel*-group yang sama, dan tabel alamat MAC tidak terpengaruhi oleh kesalahan ini [13].

Etherchannel dapat digunakan pada semua level jaringan untuk membuat *link* jalur dengan *bandwidth* yang tinggi, dan digunakan dalam beberapa tipe koneksi trafik yang tinggi juga, karena *etherchannel* dapat menggunakan pengkabelan yang ada sekarang ini membuat *etherchannel* menjadi sangat terukur [1]

2.2.9 *Load balancing* dalam *Etherchannel*

Pada dasarnya *etherchannel* membuat satu jalur logik dari *link* multi fisik yang memungkinkan dapat membagi beban *bandwidth* lalu lintas antar *link* dan menambahkan redudansi jika ada *link* yang mengalami gangguan atau permasalahan yang lainnya. *Etherchannel* digunakan untuk menghubungkan peranglat Local Area *Network* (LAN) melalui kabel fiber (single -mode dan multi-mode), dan *Unshielded Twisted Pair* [14]

Load balance etherchannel mendistribusikan lalu lintas di antara jalur *link* yang aktif, dimana setiap *link* yang dibuat dipilih menggunakan algoritma yang dibuat oleh cisco yang dinamakan algoritma hash. Algoritma ini memutuskan kemana setiap trafik harus mengirim sesuai dengan sumber atau tujuan alamat MAC, alamat IP atau nomor *port*-nya. Algoritma memberikan angka nol sampai tujuh. Tabel 2.1 akan menunjukkan bagaimana 8 angka didistribusikan di antara 2 hingga 8 *port* fisik [13].

Dalam hipotesis algoritma hash acak nyata, konfigurasi 2, 4 atau 8 *port* mengarah pada penyeimbangan beban atau *fair load balancing*, sedangkan konfigurasi lainnya mengarah pada *unfair load balancing.* Tabel 2.1 akan menunjukkan distribusi dari *load balance* dalam teknologi *port-channel.*[12]

Tabel 2. 1 Distribusi *Load Balance* di Teknologi *Port-Channel*

Nomor *Port Etherchannel*	Rasio *Load balancing* Antara Nomor *Port*
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

Switch menggunakan per-*flow balancing* karena hal tersebut merupakan bagaimana sebuah perangkat keras bekerja. Ketika *switch* menerima paket akan membuat sebuah hasil hash yang terletak di header alamat MAC sumber atau tujuan, alamat IP sumber atau tujuan ataupun nomor *port* dari sumber atau tujuan. Dari bidang mana perangkat membuat hash tergantung pada ASIC tertentu. Tidak semua *switch* dibuat sama. Perangkat lunak menggunakan hash tersebut untuk membuat keputusan mengenai *port* mana (*port* fisik) yang mengirimkan paket ke perangkat lain [14].

Algoritma hash *cisco-proprietary* menghitung nilai dalam kisaran 0 hingga 7. Nilai tersebut digunakan sebagai dasar sebuh *port* tertentu di *etherchannel* dipilih. Pengaturan *port* mencakup sebuah *mask* yang menunjukan

nilai mana yang diterima *port* untuk melakukan transmisi data. Dengan jumlah maksimum *port* dalam satu *etherchannel* yaitu delapan *port* setiap *port* hanya menerima satu nilai. Jika ada empat *port* di *etherchannel*, setiap *port* menerima dua nilai, dan seterusnya. Tabel 2.2 dibawah mencantumkan rasio nilai yang diterima setiap *port*, yang bergantung pada jumlah *port* di *etherchannel* [2].

Tabel 2. 2 *Load balancing*

No. *Port*	*Load balancing*								Nilai
1	8								8
2	4	4							8
3	3	3	2						8
4	2	2	2	2					8
5	2	2	2	1	1				8
6	2	2	1	1	1	1			8
7	2	1	1	1	1	1	1		8
8	1	1	1	1	1	1	1	1	8

2.2.10 LACP

Link Aggregation Control Protocol merupakan bagian dari spesifikasi IEEE 802.3ad yang mengijinkan pengguna untuk menggabungkan beberapa *port* fisikal bersama menjadi sebuah *channel* logika tunggal. LACP mengijinkan *switch* untuk bernegosiasi secara otomatis untuk penggabungannya dengan mengirimkan paket LACP kepada *peer*-nya. Hal ini merupakan fungsi yang sama dengan *Port Aggregation Protocol* (PAgP) dengan Etherchannel cisco.

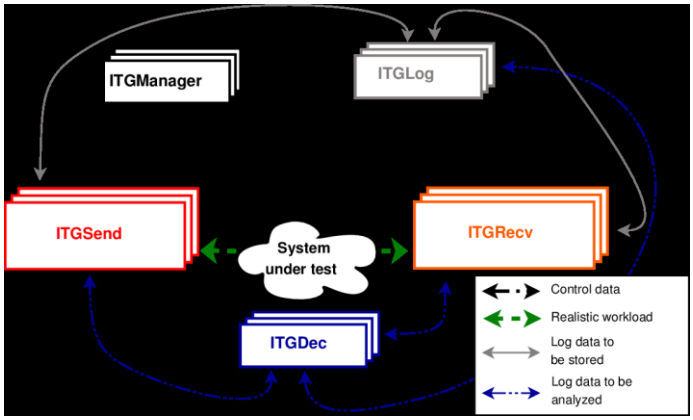
Standar IEEE 802.3ad membentuk *link layer* 2 tunggal secara otomatis dari dua atau lebih *link* ethernet menggunakan LACP. Protokol ini membuat kedua *link* ethernet akhir dapat berfungsi dan diijinkan untuk menjadi anggota dari kelompok agregasi sebelum *link* ditambahkan pada grup tersebut. LACP harus diaktifkan di kedua *link* akhir untuk bisa bekerja. Bila LACP tidak tersedia pada kedua *link* akhir maka LACP akan melakukan agregasi manual yang hanya bersyarat bahwa kedua *link* akhir berfungsi. LACP menyediakan tambahan *control* dan juga penghapusan *link* fisik dari grup agregasi sehingga tidak sampai ada *frame* yang hilang atau terduplikasi. Spesifikasi dari 802.3ad juga

menyediakan agregasi manual dari pengembangan multiple *link* di antara *switch* tanpa melakukan pertukanan pesan LACP. Agregasi manual tidak lebih handal atau lebih mudah di atur bila dibandingkan pada *link* LACP yang sudah dinegosiasikan [20].

Ketika LACP *protocol* untuk sebuah *port* menyala, *port* akan menginformasikan lawannya mengenai prioritas sistem, MAC address, prioritas *port*, nomor *port*, dan kunci operasi dengan mengirimkan LACPDU. Setelah menerima informasi, lawannya akan mengakhiri perbandingan informasi dengan informasi yang diletakkan di *port* lainnya untuk memilih sebuah *port* agar bisa di agregasi grup. Kunsi operasi adalah kombinasi konfigurasi yang sudah tergenerasi dengan *protocol* LACP berdasarkan dengan konfigurasi *port* (kecepatan, duplex, konfigurasi dasar, dan kunci manajemen) ketika *port* sudah teragregasi. Setelah LACP *protocol* diaktifkan pada *port* agregasi dinamis, kunci manajemennya menjadi default ke nol. Setelah LACP diaktifkan pada *port* agregasi statis, kunci manajemen *port* sama dengan agregasi identitas grup [15].

2.2.11 D-ITG

Distributed Internet Traffic Generator adalah sebuah platform untuk membuat trafik IPv4 dan IPv6 dengan cara menduplikasi '*workload*' dari aplikasi internet saat ini. Selain itu D-ITG juga bisa digunakan sebagai alat akur jaringan yang bisa menentukan banyak kinerja jaringan seperti *Quality of service throughput*, *delay*, *jitter*, *packet loss* dalam level paket

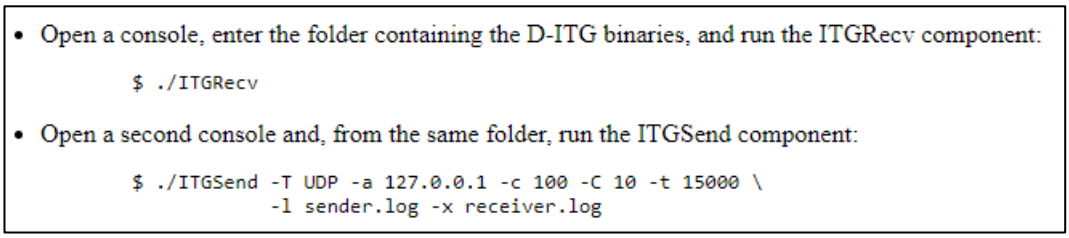


Gambar 2. 2 Arsitektur D-ITG [16]

Fitur inti D-ITG disediakan oleh *ITGSend* dan *ITGRecv*. *ITGSend* adalah komponen yang bertanggung jawab untuk menghasilkan lalu lintas menuju

ITGRecv. Memanfaatkan desain multithreaded, *ITGSend* dapat mengirim beberapa lalu lintas parallel mengalir menuju beberapa instance *ITGRecv*, dan *ITGRecv* dapat menerima beberapa arus lalu lintas paralel dari beberapa *ITGSend* instance. Saluran pensinyalan dibuat antara setiap pasangan komponen *ITGSend* dan *ITGRecv* untuk mengontrol pembangkitan semua arus lalu lintas.

D-ITG dapat digunakan sebagai alat pengukuran jaringan dengan perintah *ITGRecv* dan *ITGSend* seperti gambar 2.3



Gambar 2. 3 Cara menggunakan D-ITG [16]

Perintah tersebut dijalankan di *client* (*ITGRecv*) dan *Server* (*ITGSend*). Dari gambar tersebut *ITGSend* akan menghasilkan satu aliran UDP dengan ukuran muatan konstan (100 *byte*) dan kecepatan paket konstan (10 pps) selama 15 detik (15000 ms) dan dua file log tingkat paket akan dihasilkan baik pada pengirim (opsi -l) dan penerima (-x opsi) sisi. log lainnya dapat dilihat pada tabel 2.3 [16]

Tabel 2. 3 *Log Options*

No	*Log Options*	Keterangan
1	*-l [logfile]*	Membuat file log di sisi pengirim
2	*-x [receiver_logfile]*	Meminta *ITGRecv* untuk membuat file log di sisi penerima
3	*-t <duration>*	*Set the generation duration in ms (default: 10000 ms).*
4	*-a <dest_address>*	*Set the destination address (default: 127.0.0.1).*
5	*-T <protocol>*	*Layer 4 protocol (default: UDP)*
6	*-C <rate>*	*Constant (default: 1000 pkts/s).*
7	*-c <pkt_size>*	*Constant (default: 512 bytes).*

2.2.12 *Quality of services*

Quality of Service atau QoS (Bahasa Indonesia : kualitas layanan) mengacu pada teknologi apa pun yang mengelola lalu lintas data untuk mengurangi *packet loss* (kehilangan paket), latency, dan *Jitter* pada jaringan. QoS mengontrol dan mengelola sumber daya jaringan dengan menetapkan prioritas untuk tipe data tertentu pada jaringan. Parameter *Quality of Service* terdiri dari :

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

Tabel 2. 4 Standarisasi nilai *delay* dari TIPHON [17]

Kategori	**Delay**	**Indeks**
Poor	> 450 ms	1
Medium	300 – 450 ms	2
Good	150 – 300 ms	3
Perfect	< 150 ms	4

2. *Jitter* atau variasi kedatangan paket, diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket perjalanan *Jitter*.

Tabel 2. 5 Standarisasi nilai *jitter* dari TIPHON [17]

Kategori	**Delay**	**Indeks**
Poor	125 – 225 ms	1
Medium	75 – 125 ms	2
Good	0 – 75 ms	3
Perfect	< 0 ms	4

3. *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 [17].

Tabel 2. 6 Standarisasi nilai *throughput* dari TIPHON [17]

Kategori	**Delay**	**Indeks**
Poor	0 – 338 kbps	1
Medium	338 – 700 kbps	2
Fair	700 – 1200 kbps	3
Good	1200 – 2100 kbps	4
Perfect	> 2100 kbps	5