BAB II

LANDASAN TEORI

A. Pengertian Jaringan

Jaringan merupakan sekumpulan *hardware* yang saling terkoneksi karena adanya tembaga, kabel optic, gelombang *micro*, dan infra merah. Olehnya terjadi pertukaran data. *Hardware* yang dimaksud dapat berbentuk komputer, PDA, printer, dan *hardware* lain yang bisa melakukan transmisi data (forouzan, 2005).[1]

Jaringan komputer adalah dua atau lebih *hardware* yang saling terhubung menciptakan koneksi sehingga mampu saling menerima atau mengirim data, aplikasi, peralatan komputer, dan koneksi internet atau beberapa kombinasi tersebut (Todd, 2012, p2).[1]

Manfaat jaringan komputer untuk perusahaaan (Tanenbaum, 2003, p2) adalah :

1. *Resource Sharing*

   Memiliki tujuan nantinya semua program atau data dapat difungsikan setiap orang dilingkupnya tanpa kendala lokasi dan jarak.

2. Reliabilitas Tinggi

   Memiliki tujuan untuk menjaga keutuhan data apabila terdapat salah satu perangkatnya mengalami masalah, data tersebut dapat diambil kemudian pada perangkat yang lain.

3. Hemat Biaya

   Menggunakan komputer berukuran kecil mempunyai rasio harga atau kinerja yang lebih dibanding komputer yang besar karena komputer *mainframe* memiliki kecepatan sepuluh kali lipat dari kecepatan komputer pribadi dan harganya seribu kali lebih mahal dari komputer pribadi sehingga para perancang sistem lebih memilih membangun sistem yang terdiri dari komputer-komputer pribadi dengan menggunakan model *client- server*.

4. Skalabilitas

Untuk meningkatkan kinerja sistem secara berkala sesuai dengan beban pekerjaan dengan menambahkan sejumlah prosesor.

5. Medium Komunikasi

Dengan menggunakan jaringan dua orang atau lebih yang berjauhan dapat berkomunikasi dengan mudah.[1]

B. Internet Protocol

IP (Internet Protocol) merupakan protokol yang paling penting yang harus berada pada layer Internet *TCP/IP*. Semua protocol *TCP/IP* yang berasal dari layer mengirmkan data melalui protokol *IP* ini. Seluruh data dilewatkan, dioalah oleh protokol *IP* dan dikirimkan sebagai datagram IP untuk sampai ke sisi penerima. Dalam melakukan pengiriman data, protokol IP ini bersifat *unrealible connectionless*, dan *datagram delivery service.*

Unrealible berarti protokol *IP* yang tidak menjamin datagram yang dikirim pasti sampai ke tujuan. *Protokol IP* hanya melakukan cara terbaik untuk menyampaikan datagram yang dikirim ke tujuan. Jika pada perjalanan datagram tersebut terjadi hal-hal tidak dinginkan (putusnya jalur, kemacetan, atau sisi penerima yang dituju sedang mati), protokol *IP* hanya akan memberikan pemberitahuan pada sisi kirim kalau telah terjadi pemasalahan pengiriman data ketujuan melalui protokol *ICMP*. Sedangkan *Connectionless* berarti tidak melakukan pertukaran kontrol informasi *(handshake)* untuk membentuk koneksi sebelum mengirimkan data.

Datagram delivery service berarti setiap datagram yan dikirim tidak tergantung pada datagram lainya. Akibatnya jalur yang ditempuh oleh masing-masing datagram *IP* ketujuan bisa berbeda satu sama lainya. Dengan demikian kedatangan datagram pun bisa jadi tidak berurutan. Metode ini dipakai untuk menjamin sampainya datagram ke tujuannya walaupun salah satu jalur menuju ke tujuan mengalami masalah.

Ada juga lapisan Internet yang bertangung jawab untuk mengirimkan data melalui jaringan. Protokol lapisan Internet yang utama adalah *Internet Protocol (IP)*. *IP* merupakan protokol Internet yang mempunyai fungsi sebagai berikut: Pengalamatan, Frakmentasi datagram pada antar jaringan,

dan Pengiriman datagram antar jaringan. Diantara fungsi tersebut yang paling berkepentingan dengan administrator jaringan adalah fungsi pengalamatan. *IP* mempunyai pola pengalamatan yang unik yang membutuhkan waktu untuk membiasakanya.

Format *IP* pada terminology *TCP*/*IP*, suatu jaringan terdiri dari sekelompok host yang dapat berkomunikasi secara langsung tanpa router. Semua host *TCP*/IP yang menempati jaringan yang sam harus diberi netid yang sama. Host yang mempunyai netid harus berkomunikasi melalui router. [2]

Ada berbagai macam jenis protocol *TCP*/*IP* yang sering digunakan untuk bertukar data, antara lain seperti :

1. *Internet Control Message Protocol (ICMP)*

   ICMP (*Internet Control Message Protocol*) merupakan IP yang tidak didesain sebagai protocol yang handal. ICMP hanya bertugas untuk mengirimkan pesan-pesan khusus atau pesan-pesan kesalahan yang memerlukan perhatian, dan tidak memerlukan keamanan yang tinggi karena pengirimannya dalam bentuk datagram IP. Pesan *ICMP* ini akan dikirm jika terjadi masalah layer *IP* dan layer di atasnya (*TCP* atau *UDP*). [2]

2. *Transmission Control Protocol (TCP)*

   TCP adalah protokol yang dapat dipercaya dan dirancang untuk menyediakan alur data pada jaringan internet yang secara umum diketahui dengan kondisi tidak dapat dipercaya serta dirancang untuk beradaptasi dengan peralatan jaringan terhadap berbagai macam permasalahannya.

   Dirancangnya protokol ini untuk dapat dipercaya maka TCP bersifat *connection oriented* dalam mengirimkan data. TCP menjamin data yang terpercaya dengan menggunakan ARQ (*Automatic Repeat Request*). ARQ akan mentransmisikan secara otomatis berdasarkan informasi gagal diterimanya data *ACK* (*Acknoledgement*) dari penerima data. Untuk menjamin kontrol efektif terhadap hambatan maka

dilakukan dengan cara mengestimasi delay dari transmisi round trip time secara akurat, sehingga dengan mempergunakan informasi balasan dari jaringan tersebut maka dapat mendeteksi sebuah kemacetan jaringan dan menyelesaikannya. Penjelasan *TCP* dapat ditemui pada RFC 793, 1122, dan 1323. *TCP* memiliki tujuh fitur utama yaitu sebagai berikut:

a. *Connection oriented*, aplikasi meminta koneksi dan menggunakannya dalam transfer data.
b. *Point-to-point communication*, setiap koneksi *TCP* memiliki pasti dua titik.
c. *Reliability*, *TCP* menjamin bagi data yang dikirimkan dalam koneksi dapat terkirim dengan pasti tanpa ada yang hilang atau dobel.
d. *Full-duplex connection*, koneksi *TCP* memperbolehkan data untuk berkoneksi dari salah satu titik koneksi setiap saat.
e. *Stream interface*, *TCP* memperbolehkan aplikasi untuk mengirimkan koneksi yang berkesinambungan.
f. *Reliable startup*, membutuhkan persetujuan dari kedua aplikasi untuk melakukan koneksi baru.
g. *Graceful shutdown*, aplikasi dapat membuka aplikasi, mengirim data dan menutup koneksi serta menjamin bahwa data sampai sebelum koneksi terputus.[3]

3. User Datagram Protocol (UDP)

Protokol ini untuk mendukung konsep jaringan berbasis IP. Telah diketahui bahwa *IP* (*Internet Protocol*) sebagai protokol jaringan internet yang mengkomunikasikan dua titik jaringan serta secara spesifik semua aplikasi dan layanan terpengaruh port tetapi kondisi konsep jaringan IP tidak memberikan jaminan. Jaminan tersebut adalah jaminan bahwa data akan tersampaikan pada destination yang benar dan data tersampaikan dengan benar.[3]

Berbeda dengan *TCP*, protokol *UDP* adalah protokol yang bersifat

connectionless dalam mentransmisi data dan tidak mengenal dalam pengecekan terhadap error pengiriman data. Protokol *UDP* pada dasarnya hanya mengandung *IP* dengan tambahan header singkat. Protokol UDP tidak melakukan sebuah proses kontrol alur data, kontrol kesalahan ataupun pengiriman ulang terhadap kesalahan sehingga hanya menyediakan interface ke protokol *IP*. *UDP* sangat berguna sekali pada situasi client- server dan penjelasan *UDP* lebih detil dapat ditemui pada *RFC* 768. *UDP* memiliki karaketeristik yaitu sebagai berikut:

a. *End-to-end*, *UDP* dapat mengidentifikasi proses yang berjalan dalam komputer.
b. *Connectionless*, *UDP* memiliki paradigma *Connectionless* tanpa membuat koneksi sebelumnya dengan tanpa adanya kontrol.
c. *Message-oriented*, mengirimkan dan menerima data secara segmen.
d. *Best-effort*, yang utama adalah pengiriman yang terbaik.
e. *Arbitrary interaction*, *UDP* dapat menerima dan mengirim dari banyak proses.
f. *Operating system independent*, berdiri sendiri dalam operating system.[3]

C. Routing Protocol

Routing protokol adalah aturan atau cara pencarian jalur terbaik yang digunakan untuk mengirimkan paket data dari node pengirim ke node penerima. Paket akan melewati beberapa node penghubung, dimana protokol *routing* berfungsi untuk mencarikan jalur yang terbaik dari beberapa jalur yang akan dilalui melalui mekanisme pembentukan tabel routing (Sing, 2010).[4]

Routing protokol sendiri dibagi menjadi 2 berdasarkan karakteristiknya, yaitu: Routing Dinamis dan Routing Statis. Routing dinamis adalah routing yang memilih rute pengiriman data berdasarkan kondisi yang ada di jaringan tersebut. Sedangkan *Routing Stati*s adalah routin**g** protokol yang memilih

rute pengiriman hanya berdasarkan rute yang telah ditentukan pada table routing dan hanya bisa dirubah secara manual oleh Network Adminstrator. Dengan karakteristik yang berbeda antara Routing dinamis dan Routing statis tentunya memiliki kelebihan dan kekurangannya masing-masing. Routing Dinamis memiliki kelebihan dapat beradaptasi jika suatu link pada jaringannya rusak, sedangkan routing statis tidak bisa. Routing statis akan terus mengirimkan paket melalui link yang rusak sehingga paket yang dikirimkan tidak akan pernah terkirim ke tujuan. Dengan menggunakan routing dinamis dapat mencegah terjadinya packet loss yang disebabkan oleh link yang rusak, routing dinamis akan mencari rute link lain untuk mengirimkan paket ke tujuan jika link yang seharusnya dilewati rusak.[4]

D. VPN (Virtual Private Network)

VPN atau *Virtual Private Network* adalah teknologi jaringan komputer yang memanfaatkan medi komunikasi publik (*open connection* atau *virtual circuits*), seperti Internet, untuk menghubungkan beberapa jaringan lokal. Informasi yang berasal dari node-node *VPN* akan "dibungkus" (tunneled) dan kemudian mengalir melalui jaringan publik. Sehingga informasi menjadi aman dan tidak mudah dibaca oleh orang lain.

Umumnya *VPN* diimplementasikan oleh lembaga/perusahaan besar. Biasanya perusahaan semacam ini memiliki kantor cabang yang cukup jauh dari kantor pusat. Sehingga diperlukan solusi yang tepat untuk mengatasi keterbatasan *LAN*. *VPN* dapat menjadi pilihan yang cukup tepat. Tentu saja *VPN* bisa diimplementasikan oleh pengguna rumah atau oleh siapa pun yang membutuhkannya.[5]

Protocol yang digunakan pada objek penelitian ini yakni menggunakan *OpenVpn*; *OpenVPN* merupakan salah satu tipe *VPN* untuk interkoneksi jaringan lokal yang memanfaatkan jaringan public (*WAN*/Internet) dengan komunikasi yang bersifat secure. *VPN* ini biasa digunakan ketika dibutuhkan keamanan data yang tinggi. Secara default, *OpenVPN* menggunakan *UDP* port 1194 dan dibutuhkan certificate pada masing-masing perangkat untuk bisa terkoneksi. Untuk *client compatibility*,

OpenVPN bisa dibangun hampir pada semua *Operating System* dengan bantuan aplikasi pihak ketiga. *OpenVPN* menggunakan algoritma sha1 dan md5 untuk proses autentikasi, dan menggunakan beberapa chiper yaitu *blowfish128, aes128, aes192* dan *aes256*. Trafik yang melewati tunnel OpenVPN akan mengalami *overhead* 16%.[6]

E. QOS (Quality Of Service)

Quality of Service (*QoS*) adalah kemampuan sebuah jaringan untuk menyediakan layanan yang lebih baik lagi bagi layanan trafik yang melewatinya. *QOS* merupakan sebuah sistem arsitektur *end to end* dan bukan merupakan sebuah *feature* yang dimiliki oleh jaringan. *Quality* of Servicesuatu network merujuk ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. *Quality of Service* digunakan untuk mengukur tingkat kualitas koneksi jaringan *TCP*/*IP* internet atau intranet.[5]

Dari segi *networking*, *QOS* mengacu kepada kemampuan memberikan pelayanan berbeda kepada lalu lintas jaringan dengan kelas-kelas yang berbeda. Tujuan akhir dari *QOS* adalah memberikan network service yang lebih baik dan terencana dengan *dedicated bandwith*, *jitter*, dan *latency* yang terkontrol dan meningkatkan *loss* karakteristik.[7]

Fungsi-fungsi QoS dijelaskan sebagai berikut:

1. Pengkelasan paket untuk menyediakan pelayanan yang berbeda-beda untuk kelas paket yang berbeda-beda.
2. Penanganan kongesti untuk memenuhi dan menangani kebutuhan layanan yang berbeda- beda.
3. Pengendalian lalu lintas paket untuk membatasi dan mengendalikan pengiriman paket- paket data.
4. Pensinyalan untuk mengendalikan fungsifungsi perangkat yang mendukung komunikasi di dalam jaringan IP.[8]

QOS (Quality of Services) memiliki *standard* salah satunya adalah *THIPON (Telecomunications and Internet Protocol Harmonization Over Network)* TR.101329.V2.1.1.1999-06 yang dikeluarkan oleh *ETSI*

(European Telecommunications Standards Institude).

1. *Throughput*

Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama *interval* waktu tertentu dibagi oleh durasi interval waktu tersebut. *Throughput* merupakan kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* selalu dikaitkan dengan bandwidth karena *throughput* memang bisa disebut juga dengan *bandwidth* dalam kondisi yang sebenarnya.[8]

Bandwidth lebih bersifat fix sementara throughput sifatnya adalah dinamis tergantung trafik yang sedang terjadi.[8]

Persamaan untuk menghitung throughput adalah :

$$Throughput = \frac{Paket\ data\ diterima}{Lama\ pengamatan}$$

$$Throughput = \frac{Throughput}{Bandwith\ Total} x\ 100$$

Tabel E. 1 Kategoti Throughput

Kategori Throughput	Indeks	Throughput
Sangat Bagus	76%-100%	4
Bagus	51%-75%	3
Sedang	26%-50%	2
Buruk	<25%	1

(Sumber: ETSI 1999-2006)

2. *Packet Loss*

Packet loss didefinisikan sebagai kegagalan transmisi paket IP mencapai tujuannya. Kegagalan paket tersebut mencapai tujuan, dapat disebabkan oleh beberapa kemungkinkan, diantaranya yaitu:

a. Terjadinya overload trafik didalam jaringan.

b. Tabrakan (congestion) dalam jaringan.

c. Error yang terjadi pada media fisik.

d. Kegagalan yang terjadi pada sisi penerima antara lain bisa disebabkan karena overflow yang terjadi pada buffer. Di dalam implementasi jaringan IP, nilai paket loss ini diharapkan mempunyai nilai yang minimum.[8]

Persamaan untuk menghitung packet loss adalah :

$$Packet\ Loss = \frac{Paket\ dikirim - paket\ diterima}{paket\ yang\ diterima} x\ 100\%$$

Tabel E. 2 Kategori Packet Loss

Kategori Degredasi	Packet Loss	Indeks
Sangat Bagus	0%-2%	4
Bagus	3%-14%	3
Sedang	15%-24%	2
Buruk	>25%	1

(Sumber: ETSI 1999-2006)

3. Delay

Delay adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Delay di dalam jaringan dapat digolongkan sebagai berikut:

a. Packetization delay

Delay yang disebabkan oleh waktu yang diperlukan untuk proses pembentukan paket IP dari informasi user. Delay ini hanya terjadi sekali saja, yaitu di sumber informasi.

b. Queuing delay

Delay ini disebabkan oleh waktu proses yang diperlukan oleh router dalam menangani transmisi paket di jaringan. Umumnya delay ini sangat kecil, kurang lebih sekitar 100 micro second.

c. Delay propagasi

Proses perjalanan informasi selama di dalam media transmisi, misalnya kabel SDH, coax atau tembaga, menyebabkan delay yang

disebut dengan *delay propagasi.*[8]

Persamaan untuk menghitung delay adalah :

$$Delay\ rata\ rata = \frac{Total\ Delay}{Total\ paket\ yang\ diterima}$$

Tabel E. 3 Tabel Kategori Delay

Kategori Degredasi	**Packet Loss**	**Indeks**
Sangat Bagus	< 150 ms	4
Bagus	150 ms s.d 300 ms	3
Sedang	300 ms s.d 450 ms	2
Buruk	> 450 ms	1

(Sumber: ETSI 1999-2006)

4. Jitter

Jitter merupakan variasi delay antar paket yang terjadi pada jaringan IP. Besarnya nilai jitter akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan IP. Semakin besar beban trafik di dalam jaringan akan menyebabkan semakin besar pula peluang terjadinya congestion dengan demikian nilai jitter akan semakin besar. Semakin besar nilai jitter akan mengakibatkan nilai QoS akan semakin turun. Untuk mendapatkan nilai QoS jaringan yang baik, nilai jitter harus dijaga seminimum mungkin. Semakin kecil nilai jitter akan semakin bagus. Nilai minus pada jitter yang terjadi akibat adanya gangguan paket sehingga jarak antara 2 paket tidak sama,jika delay waktunya lebih banyak maka jitter akan bernilai positif, jika delay waktunya lebih sedikit maka nilai jitter akan negatif.[8]

Persamaan untuk menghitung delay adalah :

$$Jitter = \frac{Total\ Variasi\ Delay}{Total\ paket\ yang\ diterima}$$

Total variasi delay diperoleh dari :

$$Total\ Variasi\ Delay = Delay - Rerata\ Delay$$

Tabel E. 4 Tabel Kategori Jitter

Kategori Degradasi	Peak Jitter	Indeks
Sangat Bagus	0 ms	4
Bagus	1 s/d 75 ms	3
Sedang	76 s/d 125	2

F. Mikrotik Router OS

Mikrotik adalah sistem operasi independen berbasis Linux, khusus untuk komputer yang berfungsi sebagai router. Mikrotik sangat baik untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan berskala kecil hingga yang kompleks.[9]

Berdasarkan fungsi dan bentuknya, mikrotik dibedakan menjadi 2 jenis, yaitu:

1. Mikrotik router OS yang berbentuk perangkat lunak (software), yang dapat di-download di www.mikrotik.com dan dapat diinstal pada komputer PC.
2. Built-in Hardware Mikrotik yang berbentuk perangkat keras (hardware), yang dikemas dalam board router yang didalamnya sudah terinstal mikrotik router OS.

Mikrotik bukan perangkat lunak yang gratis jika ingin dimanfaatkan secara penuh. Dibutuhkan lisensi dari mikrotik untuk menggunakan dengan membayar. Mikrotik dikenal dengan istilah level pada lisensinya, mulai level 0 kemudian 1, 3, hingga 6. Setiap level memiliki kemampuan yang berbeda sesuai harganya. Penjelasan setiap level mikrotik sebagai berikut:

1. Level 0 (gratis). Level ini tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
2. Level 1 (demo). Pada level ini user dapat menggunakannya sebagai

routing standar dengan 1 pengaturan, dan tidak memiliki limitasi waktu untuk menggunakannya.

3. Level 3. Level ini mencakup level 1 ditambah n kemampuan untuk memanajemen hardware berbasis kartu jaringan atau Ethernet dan pengelolan perangkat wireless tipe client.
4. Level 4. Level ini mencakup level 1 dan 3 ditambah kemampuan untuk mengelola perangkat wireless tipe access point.
5. Level 5. Level ini mencakup level 1, 3, dan 4 ditambah kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
6. Level 6. Level ini mencakup semua Level dan tidak memiliki limitasi atau batasan apapun.[9]

G. Network Simulator GNS3

GNS3 adalah sebuah program *graphical network simulator* yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan simulator lainnya. Program ini dapat dijalankan di berbagai sistem operasi, seperti Windows, Linux, atau MacOS X. Untuk memungkinkan simulasi lengkap, GNS3 memiliki beberapa komponen yaitu:

1. *Dynamips* merupakan software yang dibuat oleh Christophe Fillot. Software ini untuk mensimulaikan IOS router Cisco seri 1700, 2600, 3600, 3700, dan 7200. Dynamips dikembangkan untuk keperluan *training, testing,* eksperimen, dan menguji kualitas konfigurasi IOS pada router secara real. Software ini berbasis CLI dan tidak memiliki mode GUI sehingga harus memahami perintah-perintahnya. *Dynamips* mampu berjalan dibeberapa sistem operasi seperti linux dan windows.
2. *Dynagen* dibuat oleh Greg Anuzelli merupakan program *front-end* untuk *dynamips* yang berfungsi untuk menyederhanakan konfigurasi *dynamips.*
3. Untuk membuat suatu simulasi jaringan di GNS3 terkadang kita memerlukan keberadaan *end user device* untuk keperluan test koneksi *end to end* sehingga simulasi routing menjadi terasa lebih realistis. Qemu merupakan aplikasi emulator yang mengandalkan translasi

binary untuk mencapai kecepatan yang layak saat berjalan di arsitektur komputer host. Dalam hubungannya dengan komputer host, Qemu menyediakan satu perangkat model yang memungkinkan untuk menjalankan berbagai sistem operasi yang belum dimodifikasi sehingga dapat ditampilkan dalam *hosted virtual machine monitor*. Qemu juga dapat memberikan dukungan percepatan modus campuran binary translation (untuk kernel code) dan *native execution* (untuk *user code*).[10]

4. *WinPcap* adalah tool standar yang digunakan pada industri untuk mengakses *link-layer network* pada lingkungan kerja Windows. WinPCap mengizinkan aplikasi untuk mengambil dan mentransmisikan paket-paket jaringan, serta mendukung *kernel-level packet filtering, network statistics engine*, dan *remote packet capture.*
5. Merupakan *emulator PC/node*. Prinsip kerja dari GNS3 adalah mengemulasi Cisco IOS pada komputer, sehingga PC dapat berfungsi layaknya sebuah atau beberapa router bahkan switch, dengan cara mengaktifkan fungsi dari *EthernetSwitch Card.*

Fitur-fitur yang didukung GNS3 antara lain:

1. Desain jaringan kualitas tinggi dan topologi jaringan yang kompleks.
2. Mengemulasikan berbagai *platform Cisco IOS router, IPS, PIX dan ASA firewall, JUNOS.*
3. Simulasi Ethernet sederhana, ATM dan *Frame Relay switch.*
4. Koneksi antara jaringan simulasi dengan jaringan yang sesungguhnya di dunia nyata.
5. Dapat dihubungkan ke jaringan fisik.
6. Dapat diintegrasikan dengan *Wireshark (tools packet capture/analyzer)* untuk analisa *traffic jaringan.*[10]

H. Wireshark

Wireshark adalah salah satu analisis paket bebas serta sumber terbuka.

Perangkat ini untuk digunakan sebagai pemecah suatu permasalahan jaringan, analisis, perangkat lunak dan serta mengembangkan protokol komunikasi, dan juga pendidikan, dari sekian banyak aplikasi *Network Analyzer* yang banyak digunakan oleh *Network Administrator* untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang di kelola Wireshark. Wireshark mampu menangkap paket-paket data yang ada pada jaringan tersebut. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa.[11]

Ada beberapa fitur Wireshark :

1. Berjalan pada sistem operasi Linux dan Windows.
2. Menangkap paket (*Capturing Packet*) langsung dari *network interface.*
3. Mampu menampilkan hasil tangkapan dengan detail.
4. Dapat melakukan pemfilteran paket.
5. Hasil tangkapan dapat di save, di import dan di export.[12]

I. Hardware In The Loop Simulations (HILS)

Perancangan simulasi dibagi menjadi dua tipe metode, yaitu *Model in The Loop (MIL) dan Hardware in The Loop (MIL).* MIL adalah langkah awal dari *model design controller*. MIL merupakan tingkat integrasi pertama dan didasarkan pada model sistem itu sendiri. (Turlea, 2018). MIL juga mengesankan respon global sehubungan dengan stabilitas dan penyesuaian model yang diinginkan. Pengujian *Model in The Loop* merupakan metode dimana objek uji dibagi menjadi dua bagian yaitu, bagian fisik dan bagian simulasi. Dan bagian ini terhubung membentuk gabungan fisik *numeric.* (Plummer, 2016).

HIL adalah teknik pengujian dinamis yang mensimulasikan input/output perilaku dari sistem fisik yang di interface ke sistem kontrol. Pengujian HIL memungkinkan desainer untuk mensimulasikan perilaku *real-time* dan karakteristik dari sistem, sehingga untuk menguji perangkat *Device Under Test* (DUT) yang beroperasi pada sistem fisik, tanpa perlu

perangkat keras yang sebenarnya atau lingkungan operasional. (Aravind Krishnan B, 2017). HIL berguna untuk validasi skema koordinasi perlindungan di antara perangkat perlindungan tegangan rendah. (Luca Bertoletti, 2017). Sistem HIL dapat meningkatkan kecepatan pengujian. (Oscar Goñi, 2014).[13]