BAB II

LANDASAN TEORI

2.1. Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan yang lainnya menggunakan *protocol* komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama (Anjik, 2008). Jaringan komputer dapat diartikan juga sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri lebih dari satu komputer yang saling berhubungan (Tanenbaun, 1997). Jaringan komputer pada umumnya adalah hubungan banyak komputer ke satu atau beberapa *server*. *Server* adalah komputer yang berfungsi sebagai "pelayan" pengiriman data atau penerima data serta mengatur pengiriman dan penerimaan data di antara komputer-komputer yang tersambung.

Jaringan komputer dibangun untuk membawa informasi secara tepat tanpa adanya kesalahan dari sisi pengirim (*transmitter*) maupun sisi penerima (*receiver*) melalui media komunikasi. Kendala – kendala yang muncul adalah pada media komunikasi misalnya masih mahalnya fasilitas komunikasi yang tersedia dan bagaimana pemanfaatan jaringan komunikasi lebih efektif dan efisien, serta masih terdapatnya berbagai macam gangguan saat data di transmisikan.

Jaringan komputer mempunyai beberapa manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri, karena jaringan komputer memungkinkan manajemen sumber daya lebih efisien.

2.1.1. Protokol

Protokol adalah sebuah aturan yang mendefinisikan beberapa fungsi yang ada dalam sebuah jaringan komputer, misalnya mengirim pesan, data, informasi, dan fungsi lain yang harus dipenuhi oleh pengirim (*transmitter*) dan penerima (*receiver*) agar komunikasi dapat berlangsung dengan benar (Anjik, 2008). Selain itu, protokol juga berfungsi agar komputer yang berada dalam jaringan berkomunikasi dengan bahasa yang sama.

Secara umum, fungsi protokol adalah menghubungkan pengirim dan penerima dalam berkomunikasi serta dalam bertukar informasi agar dapat berjalan dengan baik dan akurat. Fungsi protokol secara detail adalah sebagai berikut :

1. *Fragmentasi* dan *reassembly*

   Fragmentasi adalah membagi informasi yang dikirim menjadi beberapa paket data. Proses ini terjadi di sisi pengirim informasi. *Reassembly* adalah proses menggabungkan lagi paket-paket tersebut menjadi satu paket lengkap. Proses ini terjadi di sisi penerima informasi.

2. *Encapsulation*

   Fungsi dari *encapsulation* adalah melengkapi berita yang dikirimkan dengan *address*, kode-kode koreksi, dan lain-lain.

3. *Connection Control*

   Fungsi dari *connection control* adalah membangun hubungan komunikasi dari *transmitter* ke *receiver* termasuk dalam pengiriman data dan mengakhiri hubungan.

4. *Flow Control*

   Flow control berfungsi mengatur perjalanan data dari *transmitter* ke *receiver*.

5. *Error Control*

   Pengiriman data tidak terlepas dari kesalahan, baik dalam proses pengiriman maupun penerimaan. Fungsi *error control* adalah mengontrol terjadinya kesalahan yang terjadi pada waktu data dikirimkan.

6. *Transmission Service*

   Fungsi *transmission service* adalah memberi pelayanan komunikasi data khususnya yang berkaitan dengan prioritas dan keamanan serta perlindungan data.

Protokol yang dipakai untuk jaringan LAN adalah protokol *Ethernet*, *Token Ring*, FDDI (*Fiber Distributed Data Interface*) dan ATM (*Asynchronous Transfer Mode*).

1. *Ethernet*

   Protokol *Ethernet* merupakan protokol LAN yang paling banyak dipkai karena berkemampuan tinggi dengan biaya yang rendah. Kecepatan yang bisa dicapai mulai dari 10 Mbps, *Fast Ethernet* 100 Mbps dan *Gigabit Ethernet* 1000 Mbps. Protokol *Ethernet* menggunakan standar spesifikasi (*Institute of Electrical and Electronics Engineers*) IEEE 802.3, bekerja berdasarkan *broadcast network*. Setiap node *(host)* menerima setiap data yang dikirim oleh node yang lain. Menggunakan metode akses yang disebut CSMA/CD (*Carrier Sense Multiple Access/ Collision Detection*). Berikut adalah tabel berbagai jenis protokol *ethernet*, kecepatan, jenis kabel, topologi, jarak maksimum dan konektor yang sering dipakai dalam LAN :

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 2.1. Tabel berbagai jenis protokol ethernet

Jenis	Frek (Mbps)	Kabel	Topologi	Jarak Maks	Konektor
10BaseT	10	Cat 3,4,5 UTP	Star	100 Meter	RJ-45
100BaseTx	100	Cat 5 UTP	Star	100 Meter	RJ-45
10Base2	10	Thin COAX RG-58	Bus	185 Meter	BNC
10Base5	10	Thin COAX RG-58	Bus	500 Meter	DIX, AUI
10BaseFL	10	Fiber Optic	Star	2000 Meter	SC, ST
100BaseFX	100	Fiber Optic	Star	412 Meter	SC, ST
1000BaseTX	1000	Cat 6 UTP	Star	100 Meter	RJ-45
1000BaseSL	1000	Fiber Optic multi mode	Star	550 Meter	SC, ST
10000BaseLX	1000	Fiber Optic single mode	Star	3000 Meter	SC, ST

Cara kerja protokol *ethernet* adalah dengan melakukan pemeriksaan apakah jaringan sedang digunakan untuk pengiriman data atau tidak. Jika tidak ada pengiriman data, maka *host* yang ada diperbolehkan menggunakan jaringan untuk pengiriman data. Jika jaringan sedang digunakan, *host* akan menunggu sampai proses pengiriman selesai. Apabila dua *host* pada saat bersamaan melakukan pengiriman data, maka terjadilah tabrakan (*collision*). Jika terjadi *collision*, kedua *host* mengirimkan sinyal jam ke jaringan dan semua *host* berhenti mengirimkan data dan kembali menunggu. Kemudian secara *random*, *host* menunggu dan mengirimkan data kembali. *Backoff alghorithm* digunakan untuk mengatur pengiriman ulang setelah terjadi tabrakan.

2. Token *Ring*

Diciptakan IBM dengan kecepatan mencapai 4 Mbps dan 16 Mbps. Komputer yang dihubungkan ke jaringan token *Ring* menggunakan *hub* khusus yang

disebut *Multi-Station Access Unit* (MSAU). MSAU memiliki *ring input port* (RI), *ring output port* dan sejumlah *port* untuk berhubungan dengan komputer. Token *ring* menggunakan metode yang disebut *Beaconing* untuk mencari kesalahan jaringan.

Hal yang perlu diperhatikan dalam menggunakan jaringan token *ring* adalah panjang lingkaran token tidak boleh lebih dari 121,2 meter untuk kabel jenis UTP. Lobe dalam token *ring* adalah kabel untuk menghubungkan suatu komputer ke port MSAU dengan panjang maksimum 45,5 meter untuk jenis UTP (*Unshielded Twisted Pair*) dan 100 meter untuk jenis STP (*Shielded Twisted Pair*).

3. FDDI

Fiber Distributed Data Interface (FDDI) adalah protokol yang menggunakan topologi lingkaran fiber optic ganda yang disebut lingkaran *primary* dan lingkaran *secondary* yang diciptakan ANSI (*American National Standards Institute*). Kedua lingkaran tersebut dapat digunakan untuk pengiriman data, namun hanya lingkaran *primary* yang biasanya dipakai sebagai jaringan utama. Lingkaran *secondary* berfungsi jika lingkaran primary mengalami kerusakan. Jaringan FDDI mempunyai kecepatan 100 Mbps melalui media fiber optic. Fiber optic yang digunakan oleh FDDI adalah kabel multi mode fiber optic tipe 62.5/125 pm. Setiap lingkaran jaringan FDDI dapat mencapai panjang 200 km dengan jumlah *workstation* maksimum sebesar 500 buah. Jarak maksimum antar *workstation* adalah 2 km. FDDI juga menyediakan sarana penggunaan kabel *copper* yang sering juga disebut *Copperstranded Distributed Data Interface* (CDDI). Keuntungan fiber optic adalah :

a. *Bandwidth* yang besar

b. Tidak terganggu oleh sinyal listrik

c. Memiliki kapasitas untuk pemakaian jarak jauh

Hubungan dari *server* atau *workstation* ke jaringan FDDI melalui suatu peralatan jaringan yang disebut *concentrator*. Ada dua jenis *concentrator*, yaitu *concentrator* tunggal yang berhubungan dengan satu lingkaran FDDI dan *concentrator* ganda yang berhubungan dengan kedua lingkaran FDDI.

4. ATM

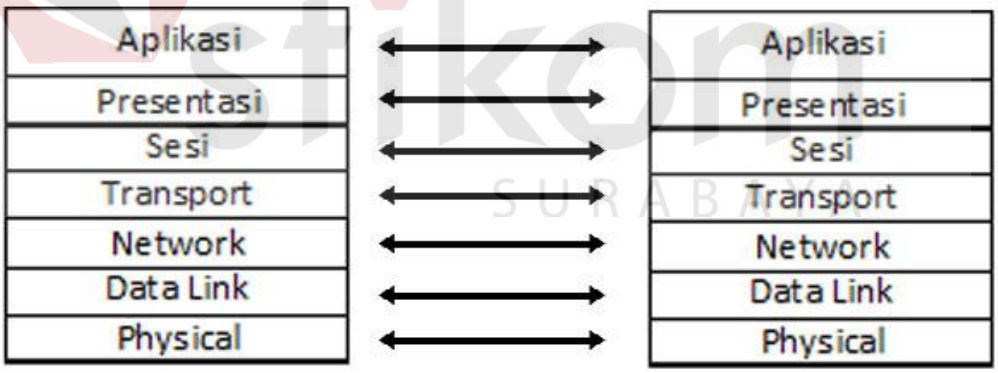
Asynchronous Transfer Mode (ATM) adalah protokol yang diatur oleh badan internasional ITU-T yang menggunakan ukuran *frame* dengan panjang tetap sebesar 53 *byte* yang disebut sel. ATM sangat cepat dan dapat memiliki *bandwidth* yang sangat besar dengan menggunakan jalur transmisi cepat seperti SONET, DS-1, OC-3, OC-12, T3, FDDI 100 Mbps, Fiber Channel 155 Mbps. Dengan menggunakan media fiber optic, kecepatannya bisa mencapai 622 Mbps. ATM juga menyediakan sarana penggunaan kabel UTP CAT-5 dengan kecepatan 155 Mbps.

2.1.2. Model Referensi OSI (*Open System Interconnection*)

OSI memberikan pandangan yang "abstrak" dari arsitektur jaringan yang dibagi dalam 7 lapisan. Model ini diciptakan berdasarkan sebuah proposal yang dibuat oleh *International Standard Organization* (ISO) sebagai langkah awal menuju standarisasi protokol internasional yang digunakan pada berbagai *layer*. Model ini disebut OSI *Reference Model*, karena model ini ditujukan untuk interkoneksi *Open System. Open System* diartikan sebagai suatu sistem yang terbuka untuk berkomunikasi dengan sistem-sistem lain yang berbeda arsitektur

maupun Sistem Operasi. Prinsip-prinsip yang digunakan bagi ketujuh *layer* tersebut adalah :

1. Sebuah *layer* harus dibuat bila diperlukan tingkat abstraksi yang berbeda.
2. Setiap *layer* harus memiliki fungsi tertentu.
3. Fungsi *layer* di bawah adalah mendukung fungsi layer diatasnya.
4. Fungsi setiap *layer* harus dipilih dengan teliti sesuai dengan ketentuan standar protokol internasional.
5. Batas-batas setiap *layer* diusahakan untuk meminimalkan aliran informasi yang melewati antarmuka.
6. Jumlah *layer* harus cukup banyak, sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam satu *layer* di luar keperluannya. Akan tetapi jumlah *layer* juga harus diusahakan sesedikit mungkin sehingga arsitektur jaringan tidak menjadi sulit dipakai.



Gambar 2.1 Komunikasi *Peer-to-peer*

Pada gambar 2.1 tampak bahwa setiap lapisan mempunyai protokol yang saling berkomunikasi *(logic)* dengan protokol pada lapisan yang sama. Data mengalir dari lapisan aplikasi ke bawah hingga lapisan fisik (disebut komunikasi vertikal), kemudian data tersebut dikirim penerima ke atas dari lapisan fisik ke

lapisan aplikasi. Masing-masing lapisan berhubungan dengan mekanisme yang disebut sebagai *Service Access Point (SAP).*

Berikut adalah penjelasan dari masing-masing *layer* pada OSI *Layer* pada Gambar 2.1.

Layer-1 (*Physical Layer*)

Physical Layer atau lapisan fisik melakukan fungsi pengiriman dan penerimaan *bit stream* dalam *medium* fisik. Dalam lapisan ini kita akan mengetahui spesifikasi mekanikal dan elektrikal dari media transmisi serta antar mukanya. Hal-hal penting yang dapat dibahas lebih jauh dalam lapisan fisik ini adalah :

1. Karakteristik fisik dari media dan antarmuka.
2. Representasi bit-bit. Dalam hal ini lapisan fisik harus mampu menerjemahkan bit 0 atau 1, termasuk pengkodean dan bagaimana mengganti sinyal 0 ke 1 atau sebaliknya.
3. *Data rate* (laju data).
4. Sinkronisasi bit.
5. *Line configuration* (konfigurasi saluran). Misalnya : *point-to-point* atau p*oint-to-multipoint configuration*.
6. Topologi fisik. Misalnya : *mesh topology*, *star topology*, *ring topology*, *bus topolog*y.
7. Mode transmisi. Misalnya : *half-duplex* mode, *full-duplex* (*simplex*) mode.

Lapisan fisik pada LAN di antaranya :

1. *Ethernet*/IEEE 802.3, *Baseband* LAN beroperasi 10 Mbps melalui kabel koaksial.

2. 100-Mbps *Ethernet (Fast Ethernet), High-speed* LAN.
3. 1000-Mbps *Ethernet (Gigabit Ethernet), High-speed* LAN.
4. *Fiber Distributed Digital Interface* (FDDI), 100-Mbps *token-passing*, *dual-ring* LAN menggunakan kabel *Fiber optic.*
5. *Token, Ring*/IEEE 802.5, *Token passing* LAN yang beroperasi pada kecepatan 4 atau 16 Mbps dengan topologi *star*.

Lapisan fisik pada WAN di antaranya :

1. *Serial Interface (async & sync)*
2. *High-speed Serial Interface (HSSI)*
3. *Protocol signal synchronous* X.21 (Jaringan X.25)

Layer-2 (*Data Link*)

Pada Layer-2 (*Data Link Layer*) komunikasi data dilakukan dengan menggunakan identitas berupa alamat simpul fisik yang disebut sebagai alamat *hardware* atau *hardware address*. Proses komunikasi antara komputer atau simpul jaringan hanya mungkin terjadi, bila kedua belah pihak mengetahui identitas masing-masing melalui alamat fisik (*physical address*). Bentuk topologi yang digunakan ditentukan oleh protokol *Data Link.* Sebagai contoh adalah BUS untuk teknologi Ethernet, RING untuk teknologi Token Ring ataupun teknologi FDDI. Selain ketiga bentuk topologi tersebut pada komunikasi serial terdapat topologi *point-to-point* atau *point-to-multipoint* pada jaringan yang menggunakan teknologi *Frame Relay* dan *ATM (Asynchronous Transfer Mode).*

Tugas utama lapisan utama data link dalam proses komunikasi data adalah :

1. *Framing* : membagi *bit stream* yang diterima dari lapisan *network* menjadi unit-unit data yang disebut *frame*.

2. *Physical Addressing*, definisi identitas pengirim dan/atau penerima yang ditambahkan dalam *header*.
3. *Flow Control* : melakukan tindakan untuk membuat stabil laju *bit* jika *rate* atau laju *bit stream* berlebih atau berkurang.
4. *Error Control* : penambahan mekanisme deteksi dan retransmisi *frame-frame* yang gagal terkirim.
5. *Communication control* : menentukan *device* yang harus dikendalikan pada saat tertentu jika ada dua koneksi yang sama.

Layer-3 (*Network Layer*)

Pada lapisan ini terjadi proses pendefinisian alamat logis (*logical addressing*), kemudian mengkombinasikan *multiple* data *link* menjadi satu *network*. Lapisan *network* bertanggung jawab untuk membawa paket dari satu simpul ke simpul lainnya dengan mengacu pada *logical address*. Fungsi lain adalah sebagai *packet forwarder* (penerus). Lapisan *Network* sebagai *packet forwarder* mengantarkan paket dari sumber (*source*) ke tujuan (*destination*) yang disebut dengan istilah *routing*.

Ada dua tugas pokok lapisan network yaitu :

1. *Logical addressing* : pengalamatan secara logis yang ditambahkan pada *header* lapisan network. Pada jaringan TCP/IP pengalamatan logis ini populer dengan sebutan *IP address*.
2. *Routing*. Hubungan antar jaringan yang membentuk *internetwork* membutuhkan metode jalur alamat agar paket dapat dikirim dari satu *device* yang berasal dari jaringan satu menuju *device* lain pada jaringan yang lain. Fungsi *routing* didukung oleh *routing protocol* yaitu protokol yang bertujuan

mencari jalan terbaik menuju tujuan dan tukar-menukar informasi tentang topologi jaringan dengan *router* yang lainnya.

Layer-4 (*Transport Layer*)

Lapisan *Transport* bertanggung jawab terhadap pengiriman *source-to-destination* (*end-to-end*) yang dapat dijelaskan sebagai berikut :

1. *Service-point Addressing*. Suatu komputer sering menjalankan berbagai macam program aplikasi ataupun *service* berlainan pada waktu bersamaan. Karena itu, *Transport Layer* tidak hanya menangani pengiriman *source-to-destination*, namun lebih spesifik kepada pengiriman jenis *message* untuk aplikasi yang berlainan. Setiap *message* yang berlainan aplikasi harus memiliki alamat tersendiri yang disebut *service point address* atau yang lebih umum disebut *port address* (port 80 = www, port 25 = SMTP).
2. *Segmentation dan Reassembly*. Sebuah *message* dibagi dalam segmen-segmen yang terkirim. Setiap segmen memiliki *sequence number* yang berguna bagi lapisan *transport* untuk merakit (*reassembly*) segmen-segmen yang terpecah menjadi *message* yang utuh.
3. *Connection Control*. Pada lapisan *transport* terdapat dua kondisi yakni *connectionless* atau *connection-oriented*. Fungsi dari *connection control* adalah mengendalikan kondisi tersebut.
4. *Flow Control*. Seperi halnya lapisan *data link*, lapisan *transport* bertanggung jawab untuk melakukan kontrol aliran (*flow kontrol*). Bedanya dengan *flow control* di lapisan *data link* adalah dilakukan untuk *end-to-end*.
5. *Error Control*. Fungsi tugas ini sama dengan tugas *error control* di lapisan *data link*, namun berorientasi e*nd-to-end*.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Dalam jaringan berbasis TCP/IP protokol yang terdapat pada lapisan ini adalah *Transmission Control Protocol* (*TCP*) dan *User Datagram Protocol* (*UDP*).

Layer-5 (*Session Layer*)

Lapisan sesi membuka, merawat, mengendalikan dan melakukan terminasi hubungan antarsimpul. Lapisan aplikasi dan presentasi melakukan *request* dan menunggu *response* yang dikoordinasikan oleh lapisan di atasnya, misalnya :

1. RPC (*Remote Procedure Call*) : Protokol yang mengeksekusi program pada komputer *remote* dan memberikan nilai balik kepada komputer lokal sebagai hasil eksekusi tersebut.
2. Netbios API : *Session Layer Application Programming Interface*.
3. NFS (*Network File System*)
4. SQL (*Structured Query Language*)

Layer-6 (*Presentation Layer*)

Berfungsi untuk mentranslasikan data yang akan ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga *Network shell* (*Virtual Network Computing* (VNC)) atau *Remote Desktop Protocol* (RDP). Lapisan presentasi melakukan *coding* dan konversi data misalnya format data untuk *image* dan *sound* (JPG, MPEG, TIFF, WAV, dan lain-lain), konversi EBCDIG-ASCII, presentasi *Big Endian* dan *Little Endian*, Kompresi, dan Enkripsi.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

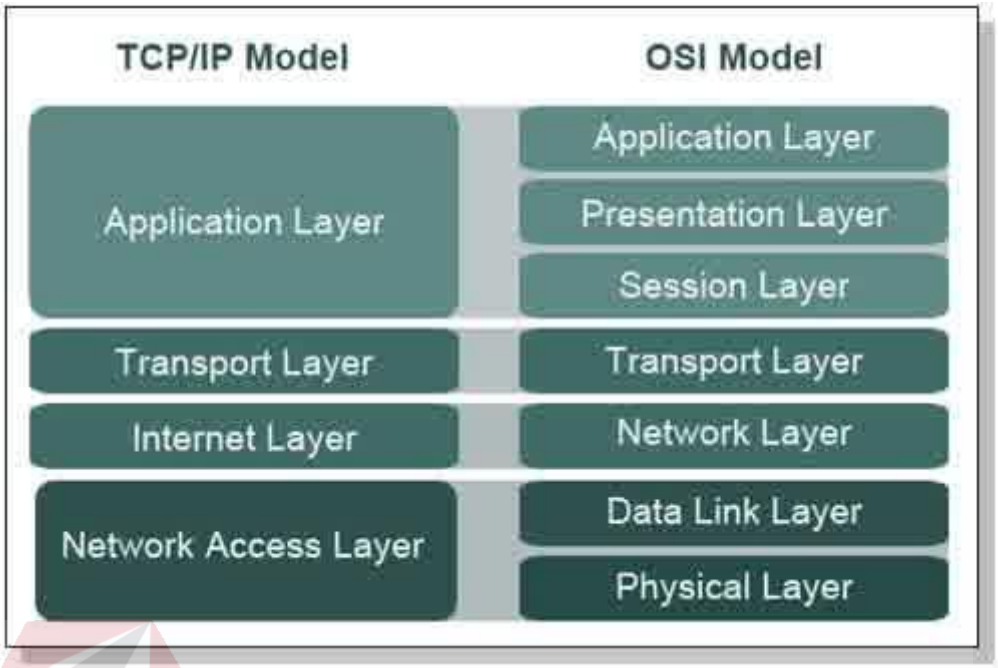
Layer-7 (*Application Layer*)

Aplikasi adalah layanan/*service* yang mengimplementasikan komunikasi antarsimpul. *Application Layer* berfungsi sebagai antamuka antara aplikasi dengan fungsionalitas jaringan yang mengatur bagaimana aplikasi dapat mengakses jaringan dan membuat pesan-pesan kesalahan. Beberapa hal yang dilakukan oleh lapisan aplikasi adalah mengidentifikasi mitra komunikasi, aplikasi transfer data, *resource availability*, dan lapisan aplikasi terkait dengan aplikasi *end-user* (Sukmaaji & Rianto 2008).

2.1.3. Model Referensi TCP/IP

TCP/IP adalah singkatan dari *Transmission Control Protocol/ Internet Protocol.* TCP bertugas menerima pesan elektronik dengan panjang sembarang dan membaginya ke dalam bagian-bagian berukuran 64 kb (kilo *bit*). Dengan membagi pesan menjadi bagian-bagian, perangkat lunak yang mengontrol komunikasi jaringan dapat mengirim tiap bagian dan menyerahkan prosedur pemeriksaan bagian demi bagian. Apabila suatu bagian mengalami kerusakan selama transmisi, maka program pengirim hanya perlu mengulang transmisi bagian itu dan tidak perlu mengulang dari awal.

IP mengambil bagian-bagian, memeriksa ketepatan bagian-bagian, pengalamatan ke sasaran yang dituju, dan memastikan apakah bagian-bagian tersebut sudah dikirim sesuai dengan urutan yang benar. IP memiliki informasi tentang berbagai skema pengalamatan yang berbeda-beda.



Gambar 2.2. TCP/IP dan OSI *Layer*

Dari gambar 2.2 dapat dilihat perbedaan *layer* antara model TCP/IP dengan model OSI (*Open System Interconnection*).

Internet Layer

Internet layer menentukan format paket dan protokol resmi yang disebut IP (*Internet Protocol*). Tugas *internet layer* adalah mengirimkan paket-paket IP yang berisi informasi tujuan paket tersebut. Di sini diperlukan *routing packet*, sebab adanya *routing packet* dapat menghindarkan terjadinya kemacetan pada waktu transmisi data. Secara tidak langsung, kita bisa melihat bahwa *internet layer* fungsinya hampir sama dengan *network layer* pada model OSI (*Open System Interconnection*).

Transport Layer

Layer yang berada di atas *internet layer* pada model TCP/IP adalah *transport layer*. Ada dua jenis *transport layer*, yaitu *Transmission Control Protocol* yang mempunyai fungsi untuk memecah data menjadi paket-paket dan

meneruskannya ke *internet layer* dan *User Datagram Protocol* yang merupakan protokol yang tidak bisa diandalkan bagi aplikasi-aplikasi yang tidak memerlukan pengurutan TCP (Sukmaaji & Rianto, 2008).

Application Layer

Model TCP/IP tidak memiki *session layer* dan *presentation layer*. *Application layer* terdapat di puncak model TCP/IP. *Layer* ini berisi bermacam-macam protokol tingkat tinggi, yaitu *telnet*, *ftp*, *smtp*, *dns*, *http*, dan *www* (Sukmaaji & Rianto, 2008).

2.2. *Social Network*

Social Network adalah istilah yang digunakan untuk menyebutkan sebuah *website* berbasis jejaring sosial, artinya suatu *website* yang memungkinkan adanya interaksi antara anggota atau pengikut dari *website* tersebut secara penuh. Saat ini *website* jejaring sosial merupakan *website* yang paling banyak mendapatkan kunjungan setelah *website search engine*, bahkan dalam beberapa kondisi tertentu *website* jejaring sosial merupakan *website* yang memiliki tingkat kunjungan tertinggi. Sebut saja *facebook*, saat ini *facebook* merupakan *website* yang paling banyak dikunjungi di beberapa negara, termasuk di Indonesia. *Facebook* merupakan situs jejaring sosial (*social network*) yang saat ini menjadi *trend* di kalangan para pengguna internet untuk mendaftarkan diri di situs jejaring sosial dan berlomba mencari relasi sebanyak mungkin.

Sementara jejaring sosial merupakan situs dimana setiap orang bisa membuat *web page* pribadi, kemudian terhubung dengan teman-teman untuk berbagi informasi dan berkomunikasi. Jejaring sosial terbesar antara lain *facebook*, *myspace* dan *twitter*. Jika media tradisional menggunakan media cetak

dan media *broadcast*, maka media sosial menggunakan *internet*. Media sosial mengajak siapa saja yang tertarik untuk berpartisipasi dengan memberi kontribusi dan *feedback* secara terbuka, memberi komentar, serta membagi informasi dalam waktu yang cepat dan tak terbatas.

Media Sosial adalah ketika aplikasi *Web* 2.0 digunakan suatu situs untuk membentuk jejaring antar-teman, biasa disebut juga situs pertemanan. Dalam suatu media sosial, anggota komunitas suatu situs tidak hanya sekedar dapat menanggapi konten atau mengirimkan konten, melainkan juga membangun relasi antar-anggota. Media sosial adalah sebuah media *online* di mana para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, *social network* atau jejaring sosial, wiki, forum dan dunia virtual. Blog, jejaring sosial dan wiki mungkin merupakan bentuk media sosial yang paling umum digunakan oleh masyarakat di seluruh dunia. Media sosial dapat didefinisikan sebagai sebuah kelompok aplikasi berbasis *internet* yang membangun di atas dasar ideologi dan teknologi *Web* 2.0, dan yang memungkinkan penciptaan dan pertukaran *user-generated content*.

Saat teknologi internet dan *mobile phone* makin maju maka media sosial pun ikut tumbuh dengan pesat. Kini untuk mengakses *facebook* atau *twitter* misalnya, bisa dilakukan dimana saja dan kapan saja hanya dengan menggunakan sebuah *mobile phone*. Demikian cepatnya orang bisa mengakses media sosial mengakibatkan terjadinya fenomena besar terhadap arus informasi tidak hanya di Negara-negara maju, tetapi juga di Indonesia. Karena kecepatannya media sosial juga mulai tampak menggantikan peranan media massa konvensional dalam menyebarkan berita-berita.

Pesatnya perkembangan media sosial kini dikarenakan semua orang seperti bisa memiliki media sendiri. Jika untuk memiliki media tradisonal seperti televisi, radio dan koran dibutuhkan modal yang besar dan tenaga kerja yang banyak, maka lain halnya dengan media sosial. Seorang pengguna media sosial bisa mengakses menggunakan media sosial dengan jaringan *internet* bahkan yang aksesnya lambat sekalipun, tanpa biaya besar, tanpa alat mahal dan dilakukan sendiri tanpa karyawan. Kita sebagai pengguna sosial media dengan bebas bisa mengedit, menambahkan, memodifikasi baik tulisan, gambar, video, grafis dan berbagai model *content* lainnya.

Menurut Antony Mayfield dari iCrossing, media sosial adalah mengenai menjadi manusia biasa. Manusia biasa yang saling membagi ide, bekerjasama dan berkolaborasi untuk menciptakan kreasi, berfikir, berdebat, menemukan orang yang bisa menjadi teman baik, menemukan pasangan, dan membangun sebuah komunitas. Intinya, menggunakan media sosial menjadikan kita sebagai diri sendiri. Selain kecepatan informasi yang bisa diakses dalam hitungan detik, menjadi diri sendiri dalam media sosial adalah alasan mengapa media sosial berkembang pesat.

Jika dalam kehidupan sehari-hari kita tidak bisa menyampaikan pendapat secara terbuka karena satu dan lain hal, maka tidak jika kita menggunakan media sosial. Kita bisa menjadi menulis apa saja yang kita mau atau kita bebas mengomentari apapun yang ditulis atau disajikan orang lain. Ini berarti komunikasi terjalin dua arah. Komunikasi ini kemudian menciptakan komunitas dengan cepat karena ada ketertarikan yang sama akan suatu hal.

Time [sec]	Action/Click	No.	Proto	Method	URI
0.000	a) open www.facebook.com				
9.944		1	HTTP	GET	/
27.696	b) login, enter password				
29.121		2	**HTTPS**	POST	/login.php?
31.012		3	HTTP	GET	/home.php?
45.513	c) open friend list				
47.631		4	HTTP	GET	/friends/?ref=tn&quickling[version]=141637;0&__ecdc=check
48.672		5	HTTP	GET	/friends/ajax/friends.php?membership=1&__ecdc=check
48.675		6	HTTP	GET	/friends/ajax/filters.php?id=XXX&__ecdc=check
56.441	d) select profile of a friend				
59.199		7	HTTP	GET	/profile.php?id=XXX&quickling[version]=141637;0&__ecdc=check
95.921	e) write "posted something on the wall" on friends wall				
97.947		8	HTTP	POST	/ajax/profile/composer.php?__ecdc=false
102.841	f) logout				
105.029		8	HTTP	GET	/logout.php?h=c909dd2db7b0a83b238ea70321d2041b&ref=mb
105.341		9	HTTP	GET	/index.php?lh=c909dd2db7b0a83b238ea70321d2041b&

Gambar 2.3. Contoh sesi interaksi *facebook*

Pada gambar 2.3, menunjukkan bagaimana contoh interaksi OSN (*Online Social Network*) pada *facebook*. *User* harus *login* sebelum memulai sesi, setelah *login user* dapat menggunakan fitur-fitur yang ada pada *facebook*. Pada akhir sesi hasil *logout* di *user* menjadi *offline*. Waktu antara *login* dan *logout* adalah sesi dimana *user* dapat menggunakan fitur-fitur *facebook*, sementara waktu sebelum *login* dan setelah *logout* adalah sesi dimana *user* tidak dapat menggunakan fitur-fitur *facebook*.

.

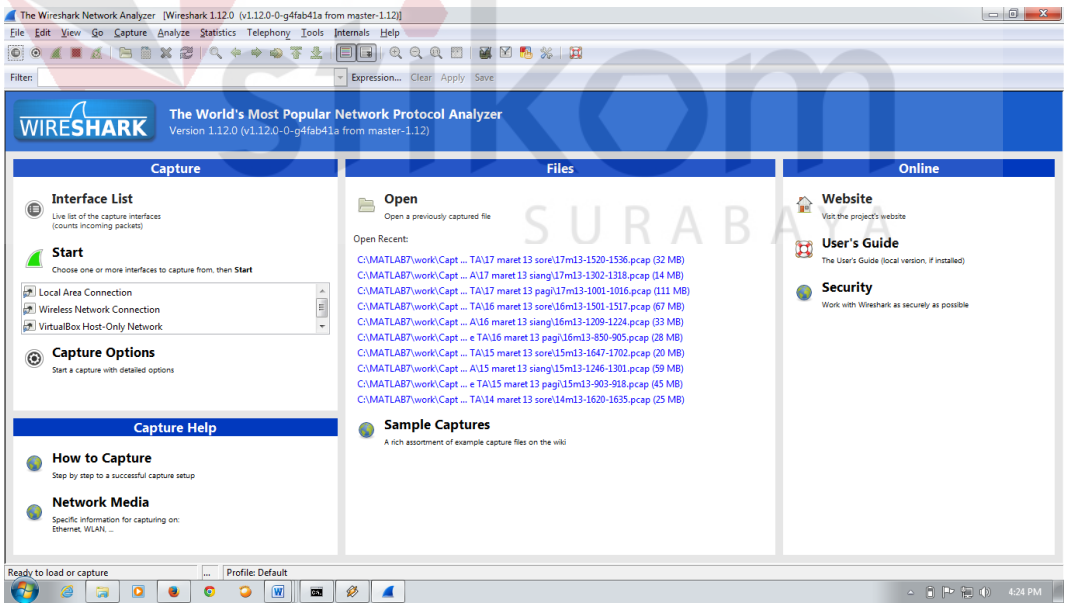
2.3. *Network Protocol Analyzer*

Protocol Analyzer adalah sebuah software yang digunakan untuk menangkap dan menganalisa sinyal dan lalu lintas data melalui saluran komunikasi yang ada. *Network Protocol Analyzer* dapat digunakan baik untuk manajemen jaringan yang sah atau untuk mencuri informasi dari jaringan. Jaringan operasi dan personil pemeliharaan menggunakan *Network Protocol Analyzer* untuk memonitor lalu lintas jaringan, menganalisis paket, menonton pemanfaatan sumber daya jaringan, melakukan analisis forensik dari pelanggaran keamanan jaringan dan memecahkan masalah jaringan. Analisa

protokol yang tidak sah bisa sangat berbahaya bagi keamanan jaringan karena mereka hampir mustahil untuk mendeteksi dan dapat dimasukkan hampir di mana saja. Adapun untuk mempercepat analisis pada paket jaringan, memerlukan sebuah *tool* yang dapat membantu proses.

2.3.1. Wireshark

Wireshark adalah *tool* yang ditujukan untuk penganalisisan paket data jaringan. *Wireshark* melakukan pengawasan paket secara waktu nyata (*real time*) dan kemudian menangkap data dan menampilkannya selengkap mungkin. *Wireshark* bisa digunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi *wireshark* dapat berjalan di banyak *platform*, seperti *linux*, *windows*, dan *mac*. Contoh aplikasi *wireshark* yang berjalan di *windows 7* tampak pada gambar 2.4.



Gambar 2.4. Tampilan aplikasi *wireshark* pada *windows 7*

Ada banyak hal yang dapat dilakukan dengan *wireshark*. Berikut adalah beberapa contoh yang mungkin menggambarkan kapan perlu menggunakan *wireshark*.

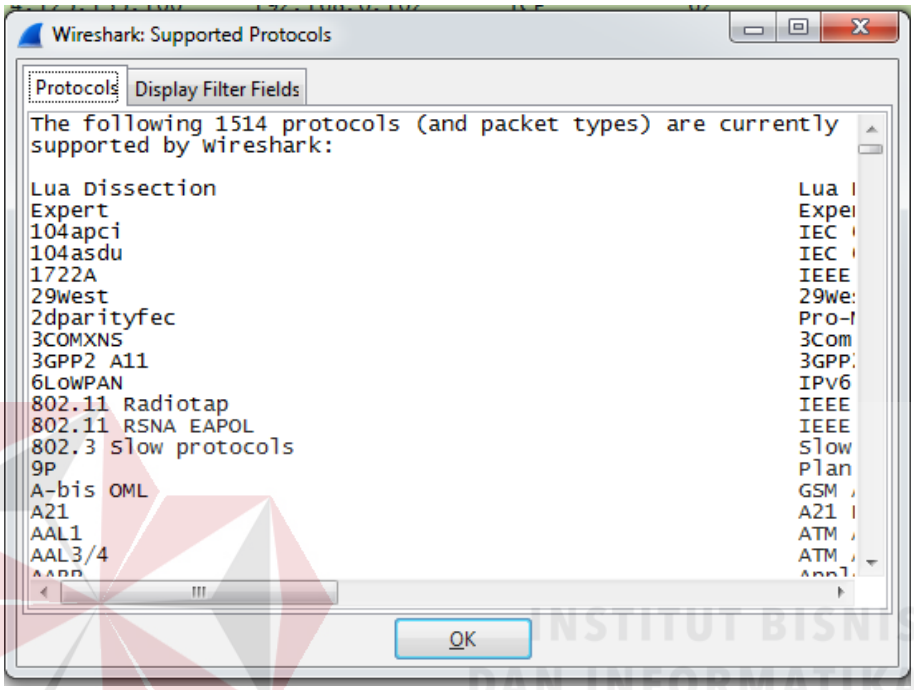
1. Melakukan *troubleshoot* permasalahan jaringan.
2. Melakukan pengujian masalah keamanan.
3. Melakukan *debugging* implementasi protokol.
4. Belajar protokol jaringan.

Wireshark ini diibaratkan sebagai media *tool* sehingga pemakaiannya diserahkan kepada penggunanya, apakah untuk kebaikan atau kejahatan. Hal ini karena *wireshark* dapat digunakan untuk mencuri informasi sensitif yang berkeliaran pada jaringan, contohnya kata sandi, *cookie*, dan sebagainya.

Wireshark dapat dikatakan sebagai *tool* analisis paket data jaringan yang paling sering digunakan. Berikut adalah sebagian fitur pada *wireshark*.

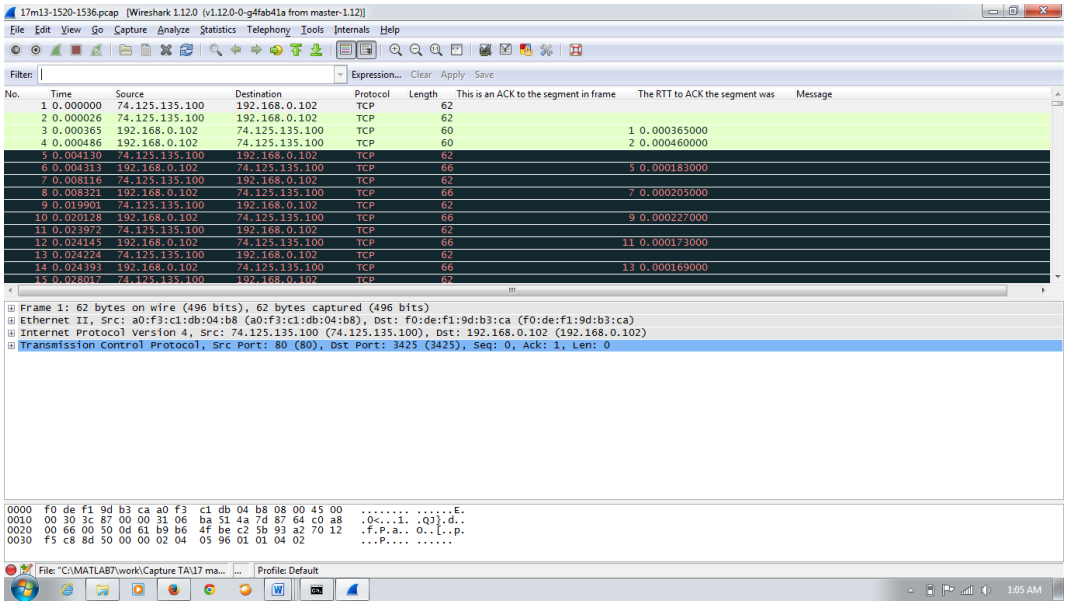
1. Tersedia untuk *platform UNIX*, *Linux*, *Windows*, dan *Mac*.
2. Dapat melakukan *capture* paket data jaringan secara *real time*.
3. Dapat menampilkan informasi protokol secara lengkap.
4. Paket data dapat disimpan menjadi file dan nantinya dapat dibuka kembali.
5. Pemfilteran paket data jaringan.
6. Pencarian paket data dengan kriteria spesifik.
7. Pewarnaan penampilan paket data sehingga mempermudah penganalisisan paket data.
8. Menampilkan data statistik.

Wireshark dapat menganalisis banyak protokol paket data jaringan. Pada *wireshark* versi 1.12.0 sudah mendukung 1514 tipe protokol yang dapat di analisis, seperti yang terlihat pada gambar 2.5.



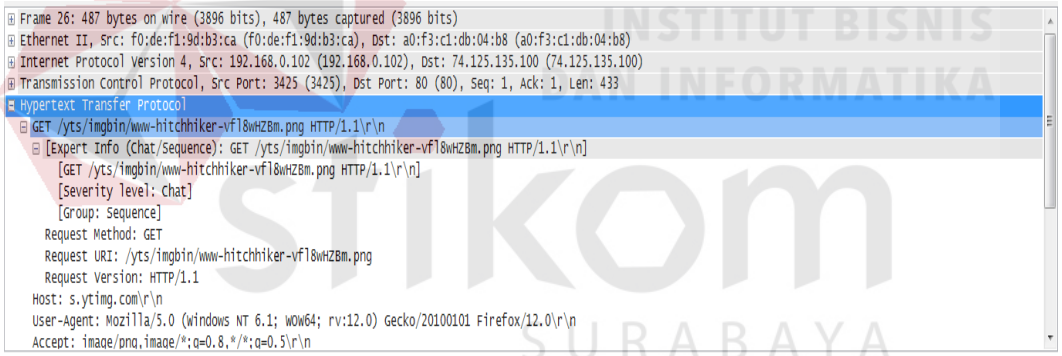
Gambar 2.5. Protokol yang didukung *Wireshark*

Wireshark dapat menganalisis paket data secara *real time*. Artinya, aplikasi *wireshark* akan mengawasi semua paket data yang keluar-masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya. Berikut contoh aplikasi *wireshark* sedang melakukan pengawasan secara real time pada gambar 2.6.



Gambar 2.6. Aplikasi *wireshark* yang mengawasi paket data secara *real time*

Paket data yang ditampilkan juga lengkap, misalnya paket data *http* yang dapat dilihat pada gambar 2.7.



Gambar 2.7. Tampilan paket data HTTP (*Hypertext Transfer Protocol*)

2.3.2. *TCPdump*

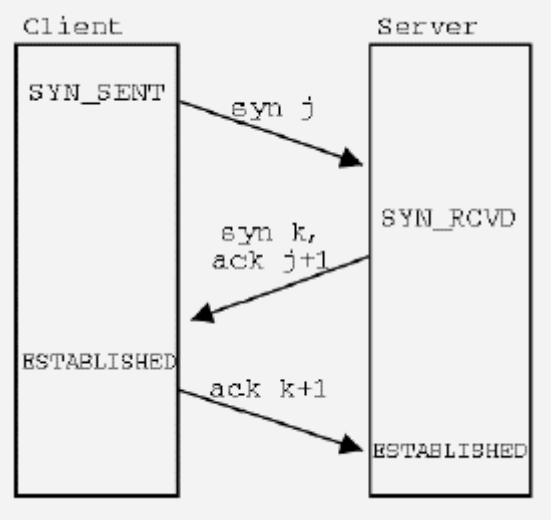
TCP/IP merupakan standar de facto untuk komunikasi antara dua komputer atau lebih. IP (*Internet Protocol*) menjalankan fungsinya pada *network layer* (pengalamatan dan *routing*) sedangkan TCP (*Transmission Control Protocol*) menyediakan jalur hubungan *end-to-end (transport layer)*.

TCPdump adalah *tools* yang berfungsi meng-*capture*, membaca atau mendumping paket yang sedang ditransmisikan melalui jalur TCP. *TCPdump* diciptakan untuk menolong *programer* ataupun administrator dalam menganalisa dan *troubleshooting* aplikasi *networking*. Seperti pisau yang bermata dua (hal ini sering kali disebut-sebut), *TCPdump* bisa digunakan untuk bertahan dan juga bisa digunakan untuk menyerang.

Utility ini juga seringkali digunakan oleh para *cracker* untuk melaksanakan perkerjaannya, karena *TCPdump* bisa meng-*capture* atau men-*sniffing* semua paket yang diterima oleh *network interface*, sama halnya dengan tujuan diciptakannya *TCPdump*.

TCPdump, utility ini juga mempunyai kemampuan untuk menganalisa PDU yang memulai dan mengakhiri suatu koneksi TCP/IP. TCP mempunyai mekanisme khusus untuk membuka dan menutup suatu koneksi. Untuk menjamin bahwa *startup* dan *shutdown* koneksi benar-benar terjadi, TCP menggunakan metode dimana ada tiga pesan yang ditukar, metode ini sering juga disebut *three-way-handshake*. Berikut adalah urutan untuk memulai (*startup*) suatu koneksi seperti pada gambar 2.8 :

1. *Host* peminta (*client*) mengirimkan bendera sinkronisasi/ *synchronization flag* (SYN) dalam segmen TCP untuk membuat suatu koneksi.
2. *Host* penerima (*server*) menerima SYN flag dan mengirimkan *flag* pernyataan/ *acknowledgment flag* (ACK) kepada host peminta koneksi (*client*).
3. *Host* peminta koneksi akan menerima ACK *flag* milik (*server*) sebagai SYN *flag* dan mengembalikan SYN *flag* yang diterima sebagai ACK *flag*-nya sendiri kepada (*server*).



Gambar 2.8. Urutan untuk memulai suatu koneksi

TCPdump juga dapat menganalisa masalah lain seperti melacak terjadinya IP spoofing melalui pengenalan (*Media Access Control Address*) MAC *address*, MITM (*man in the middle attack*) ataupun IP *hijacking* (Reza, 2006).

2.4. Pengukuran QoS (*Quality of Service*)

Quality of Service (QoS) didefinisikan sebagai suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan. Pada jaringan berbasis IP, IP QoS mengacu pada performansi dari paket-paket IP yang lewat melalui satu atau lebih jaringan. QoS didesain untuk membantu *end user* menjadi lebih produktif dengan memastikan bahwa *end user* mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Parameter-parameter performansi dari jaringan IP adalah:

2.4.1. Utilisasi *Bandwidth*

Bandwidth, didefinisikan sebagai lebar jalur dari suatu kanal komunikasi. Di dalam sebuah sistem komunikasi *analog*, *bandwidth* dinyatakan dengan satuan *hertz*, sedangkan dalam sistem komunikasi *digital bandwidth* dinyatakan dalam satuan *bit per second* (bps). *Throughput* didefinisikan sebagai jumlah paket yang dapat dilewatkan melalui sebuah kanal komunikasi yang memiliki *bandwidth* tertentu dalam rentang waktu pengamatan tertentu. *Throughput* juga dinyatakan dalam satuan bps. Dalam bentuk matematis, *throughput* dapat dirumuskan sebagai :

$$Throughput = \frac{Jumlah\ data\ yang\ berhasil\ lewat\ (bit)}{Lama\ waktu\ pengamatan\ (s)} \quad (2.1)$$

Perbandingan antara jumlah data yang dilewatkan per satuan waktu (*throughput*) yang dinyatakan dalam satuan bps dengan *bandwidth* disebut sebagai utilisasi *bandwidth*. Secara matematis, utilisasi *bandwidth* yang dinyatakan dalam prosentase dapat dituliskan sebagai berikut : (Jusak, 2014)

$$utilisasi\ bandwidth = \frac{throughput}{bandwidth}\ x\ 100\% \quad (2.2)$$

2.4.2. *Delay*

Delay atau *latency* adalah waktu tunda yang dibutuhkan dalam proses transmisi data. Misalkan paket data yang berasal dari terminal A akan dikirimkan menuju ke terminal B, didalam perjalanannya, data tersebut mengalami propagasi menuju terminal B sehingga membutuhkan waktu tertentu untuk sampai ke terminal B. Selisih waktu antara paket diterima dengan waktu paket dikirim disebut sebagai *delay* atau *latency* dan dirumuskan sebagai : (Jusak, 2014)

$$Delay = Tr - Ts \quad (2.3)$$

Yang mana :

T_r = waktu penerimaan paket (detik)

T_s = waktu pengiriman paket (detik)

2.4.3. *Jitter*

Jitter adalah variasi *delay*, yaitu perbedaan selang waktu kedatangan antar paket di terminal tujuan. *Jitter* dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (*congestion*) yang ada dalam jaringan. Semakin besar beban trafik didalam jaringan akan menyebabkan semakin besar pula peluang terjadinya *congestion* dengan demikian nilai *jitter*-nya akan semakin besar (Clark, 2003).

$$jitter = \frac{total\ variasi\ delay}{total\ paket\ yang\ diterima} \quad (2.4)$$

Dimana :

Total variasi *delay* diperoleh dari penjumlahan =

(*delay*2-*delay*1)+(*delay*3-*delay*2)+...(*delay* n – *delay* (n-1))

2.4.4. *Packet Loss*

Packet loss adalah jumlah paket yang hilang saat pengiriman paket data dari sumber ke tujuan. Kualitas terbaik pada jaringan LAN/WAN didapat jika jumlah kehilangan paket data kecil. *Packet loss* dianalisis berdasarkan jumlah paket yang hilang atau gagal mencapai tujuan pada waktu paket sedang berjalan. *Ratio packet loss* dapat dirumuskan sebagai : (Jusak, 2014)

$$Ratio\ Packet\ loss = \frac{Pd}{Ps}\ x\ 100\ \% \quad (2.5)$$

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Yang mana :

P_d = jumlah paket yang mengalami drop/gagal (paket)

P_s = jumlah paket yang dikirim (paket)

Menurut *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) *packet loss* dapat dikategorikan menjadi 4. Kategori sangat bagus dengan nilai *packet loss* 0 %, kategori bagus dengan nilai *packet loss* 3%, kategori sedang dengan nilai *packet loss* 15 % dan kategori jelek dengan nilai *packet loss* diatas 25 %.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA