Arsitektur *Real-Time System* sebagai Pemantauan Jaminan QoS

Winarno Sugeng[1], Jazi Eko Istiyanto[2], Khabib Mustofa[3]
[1]Jurusan Teknik Informatika FTI ITENAS – Bandung
[2,3]Program Ilmu Komputer FMIPA UGM – Yogyakarta
E-mail : winarno@itenas.ac.id[1] , jazi@ugm.ac.id[2] , khabib@ugm.ac.id[3]

Abstract

This paper describes the design of the internet measurement with real-time. The final result of the discussion presented in this paper is proposed a real-time system architecture as monitoring the QoS guarantee. The discussion in this paper will be preceded by an understanding of: network management, network monitoring tools, real-time system, a review of QoS, QoS monitoring, QoS monitoring method and finally with the proposed architecture the QoS guarantees based real-time system.

Keywords: internet measurement, real-time, QoS guarantee

I. PENDAHULUAN

Pertukaran informasi pada jaringan komputer global (Internet) antar banyak pihak menggunakan sarana komunikasi data digital saat ini merupakan kebutuhan yang sangat utama, bahkan dapat dinyatakan sudah menjadi kebutuhan primer dari banyak lembaga, instansi, perusahaan baik besar, menengah maupun kecil.

Pengguna komunikasi menghendaki kualitas layanan yang sesuai dengan kebutuhannya. Sebagai contoh, untuk layanan VoIP dibutuhkan waktu tunda pengiriman paket suara yang sekecil mungkin, yaitu dibawah 200 *ms*, Jika waktu tunda pengiriman paket suara ini terlalu besar, maka layanan menjadi tidak diterima oleh pengguna. Hal ini dapat dibandingkan dengan layanan email atau layanan FTP yang tidak terlalu sensitif terhadap adanya waktu tunda. Untuk itu diperlukan arsitektur pemantauan jaminan QoS agar kualitas layanan pertukaran informasi sesuai dengan yang dibutuhkan.

QoS adalah teknologi yang memungkinkan administrator jaringan untuk menangani berbagai efek dari terjadinya kongesti pada lalu lintas aliran paket dari berbagai layanan untuk memanfaatkan sumber daya jaringan secara optimal, dibandingkan dengan menambah kapasitas fisik jaringan tersebut. Jadi QoS bukan menciptakan *bandwidth* melainkan mengelola agar efektif sesuai kebutuhan. [Yoa05] [Roh08]. Arsitektur jaringan berbasis IP harus dapat menyediakan berbagai layanan pengiriman data yang didukung oleh jaminan QoS, hal mana berkaitan dengan kompleksitasnya jaringan komputer global.

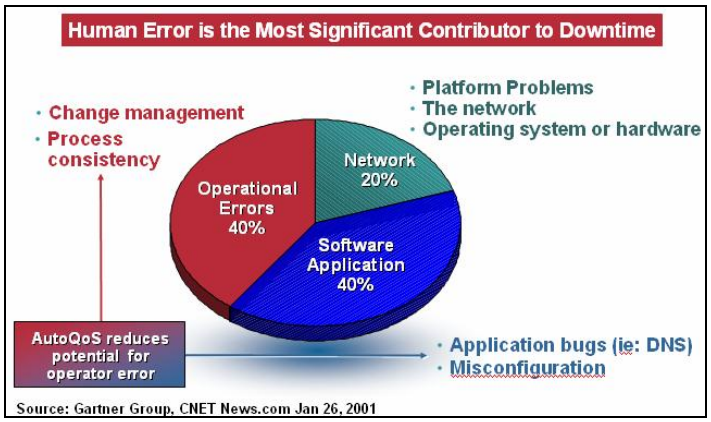
Pemantauan QoS di dalam domain-domain jaringan harus dapat ditangani dan dijaga dengan baik, sehingga manajemen QoS mutlak diperlukan, manajemen QoS yang mencakup fungsi pemantauan jaminan QoS baik untuk jaminan QoS *end-to-end*, maupun distribusi jaminan QoS di jaringan. Manajemen QoS juga menyediakan fungsi pengendalian QoS di jaringan bersekala besar. Untuk itu diperlukan suatu metoda yang mampu melakukan pemantauan jaminan QoS mengacu kepada arsitektur *real-time system.*

II. MANAJEMEN JARINGAN

Manajemen jaringan adalah kemampuan untuk memantau, mengontrol jaringan komputer dan komponen sistem jaringan. Manajemen jaringan menggunakan kekuatan Manusia dalam hal ini manajer atau pengelola jaringan, Komputer dan Jaringan Komputer untuk mengatur dan mengelola sistem serta jaringan itu sendiri. Dalam melakukan hal itu, seorang yang bertindak sebagai manajer jaringan mengandalkan berbagai macam peralatan guna terciptanya manajemen jaringan yang baik dan efisien.

Manajemen jaringan komputer saat ini menuntut harus dijaga kestabilan operasionalnya. Masalah yang terjadi pada operasional jaringan akan mengakibatkan kerugian yang tidak kecil. Masalah jaringan dapat menyebabkan *downtime* pada seluruh sistem jaringan. [KiG09]. Faktor terbesar yang menyebabkan jaringan *downtime* adalah kesalahan manusia, terlihat pada gambar 1, disamping dua faktor lainnya yaitu perangkat keras jaringan dan aplikasi perangkat lunak. Untuk mengatasi masalah yang dihadapi dan agar supaya kondisi jaringan tetap stabil, maka diperlukan adanya manajemen jaringan yang baik.

Tujuan dari pengembangan manajemen jaringan adalah memanfaatkan sumber daya yang terdapat pada suatu sistem jaringan komputer dengan semaksimal dan seefisien mungkin. Selain itu diharapkan dengan adanya manajemen jaringan suatu sistem jaringan akan lebih mudah memantau aktifitas yang ada di dalam sistem jaringan tersebut.



Gambar 1. Faktor-faktor yang sering menyebabkan jaringan *down* (cisco.com)

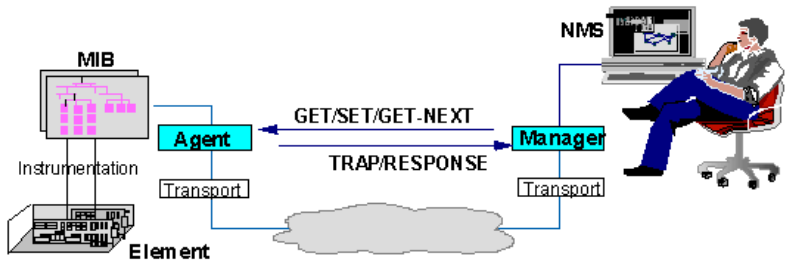
III. *NETWORK MONITORING TOOLS*

Standar dalam melakukan *Network Monitoring Tools* yang umum digunakan adalah yang pertama menggunakan SNMP *(Simple Network Management Protocol).* Yang kedua adalah dengan Penyadap Paket *(Sniffer packet)* yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer,* standar lainnya adalah dengan protokol ICMP *(Internet Control Message Protocol).* [Bud02]

SNMP merupakan protokol standar industri yang digunakan untuk memantau dan mengelola berbagai perangkat di jaringan Internet meliputi *hub, router, switch, email server, file server, workstation* dan sistem manajemen jaringan secara jarak jauh (*remote*). [Onn01]. SNMP adalah sebuah protokol yang didesain untuk memberikan kemampuan kepada pemakai untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Dengan menggunakan protokol ini dapat

diperoleh informasi tentang status dan keadaan dari suatu jaringan. Protokol ini menggunakan transport UDP pada port 161. Pengolahan dijalankan dengan mengumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola.

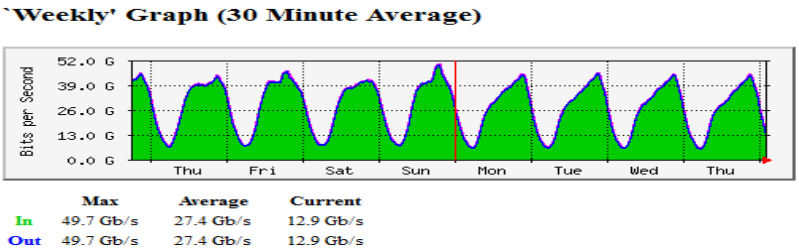
Ide dasar dari setiap manajemen jaringan adalah bahwa terdapat dua tipe sistem pada setiap jaringan yang terkonfigurasi yaitu : agen dan manajer atau NMS *(Network Management Station)*, yang terlihat pada struktur SNMP pada gambar 2, yang ditempatkan pada setiap titik pada jaringan yang akan diatur, termasuk *PC, Workstation, server, bridge, router* dan lainnya termasuk modul agen. Cara yang biasa dipakai SNMP adalah NMS mengirim permintaan *(request)* ke agen tentang informasi atau memerintahnya untuk melakukan pembaharuan keadaannya dengan cara-cara tertentu. Idealnya, agen cukup menjawab pertanyaan diminta atau dikonfirmasikan bahwa agen telah melakukan pembaharuan keadaan sesuai dengan permintaan manajer.



Gambar 2. Struktur SNMP (columbia.edu)

Semua aplikasi jaringan pada umumnya berbagi protokol manajemen jaringan yang umum. Protokol ini menyediakan fungsi-fungsi fundamental untuk mengambil informasi manajemen dari agen dan mengirimkan perintah kepada agen. Protokol ini kemudian menggunakan fasilitas komunikasi seperti TCP/IP atau OSI (*Organisasi Standar Internasional*). Akhirnya setiap agen memelihara basis informasi manajemen yang berisi informasi terbaru dan yang sebelumnya tentang konfigurasi dan lalu lintas lokalnya. Manajemen stasiun akan memelihara basis informasi manajemen global dengan informasi berisi rangkuman dari semua agen.

Aplikasi yang sangat poluler untuk membantu menganalisa traffic jaringan komputer dengan memanfaatkan aplikasi SNMP pada router adalah MRTG (*Multi Router Traffic Grapher*). MRTG merupakan aplikasi yang berguna untuk memantau penggunaan "*bandwith*" dalam suatu jaringan. Contoh aplikasi MRTG dapat dilihat pada gambar 3, dalam hal ini contoh grafik lalu lintas jaringan dalam periode mingguan.



Gambar 3. MRTG Screenshoot Weekly graph (oss.oetiker.ch)

Packet Sniffer arti tekstual 'pengendus paket' atau dapat pula diartikan 'penyadap paket', yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan terkadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan seperti hub atau switch, salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (*promiscuous mode*) untuk "mendengarkan" semuanya, yang umumnya pada jaringan kabel.

Packet Sniffer sebenarnya selain berfungsi sebagai pemantau penggunaan jaringan dan menyaring isi isi tertentu, dapat dimanfaatkan untuk mengatasi permasalahan pada jaringan komputer, mendeteksi adanya penyelundup dalam jaringan (*Network Intusion*), memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya misalkan *password*, dan dapat pula digunakan untuk *reverse engineer* pada jaringan.

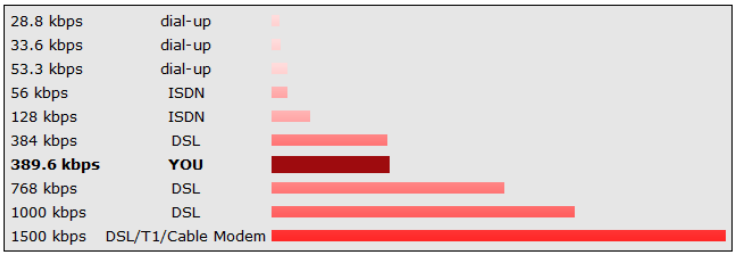
Pada umumnya manajemen jaringan untuk kebutuhan pemantauan jaringan yang menggunakan *Sniffer packet* ini untuk kebutuhan *commercial* atau *proprietary software*, berbeda halnya dengan SNMP yang berbasis *Open Source*. Hal mana melalui *Packet Sniffer* ini mampu dilakukan proses pengamatan sampai hal yang pribadi, sebagai contoh pencatatan *password* dan riwayat kegiatan yang terjadi pada terminal tertentu. Untuk itu diperlukan pertanggung jawaban khusus. Tidak semua orang dapat dengan mudah menggunakannya. Sehingga cara ini sering diterapkan untuk kebutuhan *network minitoring security*. Salah satu aplikasi adalah *Network Protocol Packet Analyzer*, yang mampu menangkap semua lalu lintas transportasi di segmen jaringan lokal dan *decode* semua hal yang sering digunakan termasuk protokol TCP/IP, UDP, HTTP, HTTPS, SMTP, POP3, TELNET, FTP, dll. Salah satu aplikasi *Packet Sniffer* terlihat pada gambar 4, nampak lebih lengkap dan kompleks dibanding aplikasi MRTG.

Gambar 4. ***Network Protocol Packet Analyzer*** (javvin.com)

ICMP *(Internet Control Message Protocol)* salah satu protokol inti dari keluarga protokol internet dan didefinisikan di dalam RFC 792. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan yang menyatakan kesalahan, sebagai contoh, bahwa komputer tujuan tidak dapat dijangkau. ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi *Ping* yang mengirim pesan ICMP *Echo*

Request dan menerima *Echo Reply* untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan.

Ping (*Packet Internet Groper*) sering digunakan untuk melakukan pengecekan apakah mesin yang dituju dalam kondisi *live* atau *no-live* dan untuk mengetahui *bandwidth* (lebar pita) dari suatu *backbone* (jalur utama) suatu jaringan yang digunakan/disewa. Pengembangan dari aplikasi ping adalah *Speedtest*, keluaran aplikasinya seperti terlihat pada gambar 5. Aplikasi ini lebih difokuskan untuk mengetahui lama transfer dari luar ke dalam (*downstream*) dan dapat juga dilengkapi transfer dari dalam ke luar (*upstream*).



Gambar 5. Tampilan *Speedtest* *(Script by derek@gambitdesign.com)*

IV. *REAL-TIME SYSTEM*

"*Real–time system*" atau dalam terjemahan bebas "Sistem waktu–nyata" begitu pesat berkembang dan aplikasinya telah meluas di berbagai bidang. *Real-time system* dapat didefinisikan sebagai sebuah sistem yang tidak hanya berorientasi terhadap hasil (*output*) yang dikeluarkan tapi di sana juga sistem dituntut untuk dapat bekerja dengan baik dalam kebutuhan waktu tertentu. Di dalam *real-time system*, waktu merupakan faktor yang sangat penting untuk diperhatikan. Faktor waktu menjadi sesuatu yang sangat kritis dan sebagai tolak ukur baik-tidaknya kinerja keseluruhan sistem tersebut. Akan tetapi, ada satu hal yang perlu diingat, *real-time system* tidak sama dengan *fast-system*. *Fast-system* adalah sistem yang bekerja dalam waktu yang sesingkat-singkatnya yang dalam artian semakin cepat *output* yang dihasilkan oleh sistem tersebut berarti semakin baik kinerjanya. Berbeda dengan *fast-system, real-time system* bekerja dalam periode dan waktu *deadline* tertentu sehingga belum tentu semakin cepat output yang dihasilkan berarti menunjukkan sistem tersebut bekerja dengan baik. Adapun contoh dari *real-time system* adalah sistem perbankan, sistem pengontrol pesawat udara, sistem otomasi pabrik, dan sebagainya. [Arw02][Bam10]

Real–time system harus menghasilkan respon yang tepat dalam batas waktu yang telah ditentukan. Jika respon komputer melewati batas waktu tersebut, maka terjadi degradasi performansi atau kegagalan sistem. Sebuah *Real-time system* adalah sistem yang kebenarannya secara logis didasarkan pada kebenaran hasil-hasil keluaran sistem dan ketepatan waktu hasil-hasil tersebut dikeluarkan. Aplikasi penggunaan sistem seperti ini adalah untuk memantau dan mengontrol peralatan seperti motor, *assembly line*, teleskop, atau instrumen lainnya. Peralatan telekomunikasi dan jaringan komputer biasanya juga membutuhkan pengendalian secara real time. Berdasarkan batasan waktu yang dimilikinya, *Real-time system* ini dibagi atas: *Hard Real time, Soft Real time, Firm Real time*. Sedangkan komponen dari *real-time system* ini adalah: Perangkat keras, Sistem Operasi *Real time*, Bahasa Pemrograman *Real Time*, Sistem Komunikasi.

V. TINJAUAN QoS

QoS atau merupakan kepanjangan dari *Quality of Service*, sebagaimana dijelaskan dalam rekomendasi CCITT E.800 adalah : "Efek kolektif dari kinerja layanan yang menentukan derajat kepuasan seorang pengguna terhadap suatu layanan". Jika dilihat dari ketersediaan suatu jaringan, terdapat karakteristik kuantitatif yang dapat dikontrol untuk menyediakan suatu layanan dengan kualitas tertentu. Karakteristik layanan tersebut adalah *delay* dan *throughput*.

Terdapat dua mekanisme dasar dalam penyediaan QoS yang memadai yang didasarkan pada nilai *delay* dan *throughput* tadi, yaitu: kapasitas yang sangat besar dan *traffic engineering*, dimana dalam *traffic engineering* terdapat dua katagori yaitu : *Reservation-based* dan *Reservation-less*.

Internet yang terus tumbuh merupakan tantangan ISP (*Internet Service Provider*) dan *network operator* untuk mempertemukan masa depan kebutuhan lalu lintas jaringan komputer global dan fitur QoS yang diharapkan. Untuk menjaga agar kompetitif, ISP dan *network operator* harus dapat memecahkan dua masalah utama : bertambahnya *backbone Internet* yang menyesuaikan kebutuhan lalul lintas yang kontinu dan menyediakan QoS yang bagus untuk lalu lintas tersebut. Dua pendekatan telah muncul untuk memecahkan problem penambahan lalu lintas internet yang kontinu. Pendekatan pertama, *IP switching*, dapat memecahkan masalah ruter yang lambat dengan menggunakan *switching* yang lebih cepat; pendekatan kedua adalah mengembangkan router yang lebih cepat.

Atas dasar tersebut diatas maka memang benar kebutuhan jaminan QoS merupakan isu yang sangat penting di jaringan global berkecepatan tinggi sekarang ini, karena pengguna komunikasi menghendaki kualitas layanan yang sesuai dengan kebutuhannya. Oleh karena itu, arsitektur jaringan berbasis IP harus dapat menyediakan berbagai layanan pengiriman data yang didukung oleh jaminan QoS, hal mana berkaitan dengan kompleksitasnya jaringan komputer global. Dengan semakin kompleksnya jaringan, masalah penyediaaan jaminan QoS yang efektif di jaringan global kecepatan tinggi manjadi hal yang sangat penting. Jaringan QoS di dalam domain-domain jaringan harus dapat ditangani dan dijaga dengan baik, sehingga manajemen QoS mutlak diperlukan, manajemen QoS yang mencakup fungsi pemantauan jaminan QoS baik untuk jaminan QoS *end-to-end*, maupun distribusi jaminan QoS di jaringan.

Seperti yang telah disinggung sebelumnya, QoS adalah teknologi yang memungkinkan administrator jaringan untuk menangani berbagai efek dari terjadinya kongesti pada lalu lintas aliran paket dari berbagai layanan untuk memanfaatkan sumber daya jaringan secara optimal, dibandingkan dengan menambah kapasitas fisik jaringan tersebut. Kebanyakan para administrator berpikir pendek jika terjadi masalah kepadatan traffic jaringan maka penyelesaiannya selalu menambah kapasitas fisik dalam hal ini lebar pita atau bandwidth layanan. Pada kenyataannya meningkatnya berbagai layanan akan meningkatkan lalu lintas aliran paket dengan berbagai laju kecepatan, yang akan membutuhkan kemampuan jaringan melalukan aliran paket pada laju kecepatan tertentu. Sebenarnya adalah yang didahulukan upaya memanfaatkan sumber daya jaringan secara optimal yang didahulukan. Ada banyak faktor-fator yang terkait dalam kasus ini sehingga menambah kapasitas fisik bukan satu-satunya jalan yang harus ditempuh.

Jaminan QoS bertujuan untuk menyediakan QoS yang berbeda-beda untuk beragam kebutuhan akan layanan di dalam jaringan IP, sebagai contoh untuk menyediakan pita lebar yang khusus, menurunkan hilangnya paket-paket, menurunkan waktu tunda dan

variasi waktu tunda di dalam proses transmisinya. Terdapat tiga metode QoS yang umum dipakai, yaitu: *Best-Effort Service, Integrated Service (IntServ),* dan *Differentiated Service (DiffServ)*. Ketiga metoda QoS tersebut dapat dijelaskan secara singkat sebagai berikut :

1. *Best Effort Service*
   Merupakan metoda QoS yang paling sederhana, tidak akan memberikan jaminan paket dapat sampai ke tujuan yang dikehendaki. Metode ini digunakan untuk melakukan semua usaha agar dapat mengirimkan sebuah paket ke suatu tujuan. Untuk aplikasi yang sensitif terhadap *network delay*, fluktuasi *bandwidth*, dan perubahan kondisi jaringan, penerapan *best-effort service* tidak dapat dilakukan. Pelayanannya merupakan pelayanan standar, pada saat ini untuk menangani aplikasi umum seperti FTP dan E-mail, dengan mengaplikasikan strategi *first in first out* (FIFO).

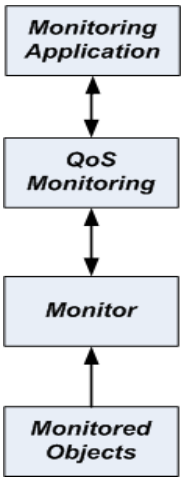
2. *Integrated Service (IntServ)*
   Merupakan metoda QoS yang menyediakan aplikasi dengan tingkat jaminan layanan melalui negosiasi parameter jaringan secara *end-to-end*.
   Aplikasi akan mengirimkan sinyal awal yang sekaligus membawa nilai QoS yang diperlukan, jadi diawali dengan cara pemesanan *bandwidth* terlebih dahulu melalui pensinyalan awal. Aplikasi tidak akan mengirimkan data lalu lintas jaringan, sebelum menerima tanda bahwa jaringan mampu menerima beban yang akan dikirimkan aplikasi dan juga mampu menyediakan QoS yang diminta secara *end-to-end*. Untuk itulah suatu jaringan akan melakukan suatu proses yang disebut *admission control* (mekanisme yang mencegah jaringan mengalami *over-loaded*.).
   Dua model layanan IntServ adalah:
   - *Guaranteed-service*, layanan dengan batas *bandwidth* dan *delay* yang jelas.
   - *Controlled-load service*, layanan dengan persentase *delay* statistik yang terjaga.

3. *Differentiated Service (DiffServ)*

   Merupakan metode QoS yang terakhir yang menyediakan suatu set perangkat klasifikasi dan mekanisme antrian terhadap protokol atau aplikasi dengan prioritas tertentu di atas jaringan yang berbeda. *DiffServ* bergantung kepada kemampuan *edge router* untuk memberikan klasifikasi dari paket-paket yang berbeda tipenya yang melewati jaringan. Lalu lintas jaringan dapat diklasifikasikan berdasarkan alamat jaringan, *protocol* dan *port, ingress interface*, atau klasifikasi lainnya selama masih didukung oleh *standard access list* atau *extended access list*. Keuntungan *Diffserv adalah Scalability, Ease of administering, Simplicity, Measurable*. Arsitektur Diffserv memiliki tiga komponen, yaitu: *Policy and resource manager, Edge routers, Core routers.*

VI. PEMANTAUAN QoS

B.Y.Jiang dkk, mengemukakan sebuah model dari sistem pemantauan QoS seperti terlihat pada gambar 6, yang komponen-komponennya terdiri dari *monitoring application, QoS monitoring, monitor dan monitored objects.* Fungsi dari komponen-komponen dapat dijelaskan dibawah ini :



Gambar 6. Model Pemantauan QoS [BYJ00]

1. *Monitoring application*, merupakan sebuah antarmuka bagi administrator jaringan. yang berfungsi mengambil informasi lalu lintas paket data dari *Monitor*, menganalisnya dan mengirimkan hasil analisis pada pengguna. Hasil analisis tersebut akan digunakan administrator jaringan sebagai dasar melakukan operasi-operasi yang lain yang diperlukan dan direkomendasikan pada jaringan yang dikelolanya.
2. *QoS monitoring*, menyediakan mekanisme pemantauan QoS dengan mengambil informasi nilai-nilai parameter QoS dari lalu lintas paket data.
3. *Monitor,* mengumpulkan dan merekam informasi lalu lintas paket data, yang selanjutnya melakukan pengukuran aliran paket data secara waktu nyata dan melaporkan hasilnya kepada *monitoring application.*
4. *Monitored Objects*, merupakan informasi seperti atribut dan aktifitas yang dipantau di dalam jaringan. Di dalam konteks pemantauan QoS, informasi-informasi tersebut merupakan aliran-aliran paket data yang dipantau secara waktu nyata. Tipe aliran paket data tersebut dapat diketahui dari *source* dan *destination* di *layer-layer* IP, port yang dipergunakan misalnya UDP atau TCP, dan parameter di dalam paket RTP.

Pemantauan QoS dapat diklasifikasikan ke dalam dua kategori yaitu pemantauan QoS dari ujung-ke-ujung *(end-to-end QoS monitoring, EtE QM)* dan pemantauan distribusi QoS per node *(distribution monitoring, DM)*. Di dalam EtE QM, pemantauan QoS dilakukan dengan cara mengukur parameter-paremeter QoS dari pengirim kepada penerima. Sedangkan di dalam DM, proses pemantauan QoS dilakukan di segmen-segmen jalur pengiriman atau antara *node-node* tertentu yang dikehendaki di sepanjang jalur pengiriman paket data. [Yoa05]

VII. METODA PEMANTAUAN QoS

Berikut ini dijelaskan beberapa metoda untuk melakukan pemantauan QoS yang dikembangkan oleh para peneliti bidang jaringan komputer :

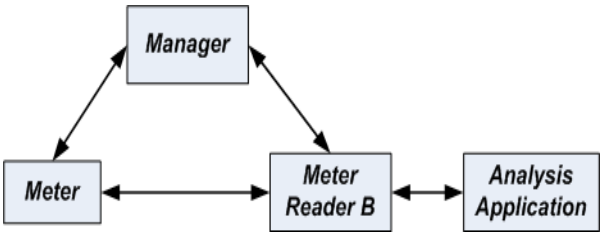
1. *Mourelatou dkk.* menjelaskan sebuah pendekatan berbasis agen untuk mengidentifikasi masalah QoS. Agen bertanggungjawab untuk melakukan pemantauan QoS dari ujung-ke-ujung. Sebuah sistem manajemen memiliki kemampuan untuk mengidentifikasi penyebab terjadinya penurunan kinerja dengan cara mengkorelasikan informasi yang

didapatkan dari agen-agen yang secara langsung memantau QoS.

2. *Chen dkk.* memperkenalkan sebuah pendekatan piranti lunak untuk melakukan pemantauan QoS di jaringan *asynchronous transfer mode (ATM).* Untuk memantau QoS dari sebuah koneksi virtual yang dipilih, sebuah koneksi paralel akan dibangun dengan rute jalur pengiriman dan nilai-nilai parameter QoS yang sama.
3. *Waldbusser* mengemukakan sistem pemantauan yang tidak terbatas hanya untuk melakukan pemantauan lalu lintas data di *layer network*, namun juga dengan melihat protokol-protokol di *layer* yang lebih tinggi yang berjalan di atas protokol *layer* network. RMON-2 memiliki kemampuan untuk melihat di atas *layer* IP dengan membaca header yang dibawa oleh level yang lebih tinggi seperti TCP dan juga header-header di *layer* aplikasi. Sebuah manajer jaringan akan menjalankan pemantauan *layer* aplikasi yang dibutuhkan untuk pemantauan QoS.
4. *Real Time Transport Control Protocol* (RTP control protocol atau RTCP) didasarkan pada transmisi periodik paket kontrol untuk semua yang terhubung dalam sesi, menggunakan mekanisme distribusi yang sama dengan paket data. Protokol yang mendasari harus menyediakan multiplexing dari paket data dan kontrol, misalnya menggunakan nomor port yang terpisah dengan UDP.
5. *Brownlee dkk*. mengusulkan sebuah arsitektur yang disebut sebagai *Real Time Flow Measurement (RTFM),* untuk melakukan pengukuran dan reporting dari aliran lalu lintas data yang dibangkitkan oleh aplikasi multimedia. Mekanisme RTFM dapat juga digunakan untuk melakukan pemantauan paket data di *layer* aplikasi.

VIII. *REAL TIME FLOW MEASUREMENT* (RTFM)

RTFM yang dikembangkan oleh *Brownlee dkk* telah menjadi dokumen IETF dari salah satu metode pemantauan QoS yang telah dikembangkan. *Realtime Traffic Flow Measurement Working Grup* mengembangkan RTFM *Traffic Measurement System* yang dideskripsikan di RFC 2064, RFC 2722, RFC 2720, RFC 2723 dan RFC 2123. Arsitektur RTFM, yang dimodelkan pada gambar 7, terdiri dari *Meter, Meter Reader, Manager,* dan data dianalisis dengan *analysis application* yang tidak ditentukan lebih lanjut dalam rekomendasi. [Yoa05]



Gambar 7. Arsitektur RTFM (RFC 2722)

Fungsi dari komponen-komponen dari Arsitektur RTFM yang direferensikan dari RFC 2722 dapat dijelaskan sebagai berikut :

1. *Manager*

   Manager merupakan aplikasi yang mengkonfigurasi *Meter* dan mengontrol *Meter Reader*. Dengan cara mengirimkan perintah konfigurasi ke *Meter* dan mengawasi operasi yang tepat dari setiap *Meter* dan *Meter Reader* agar dapat beroperasi dengan

baik. *Manager* dapat mengendalikan beberapa *Meter* dalam waktu yang bersamaan. *Manager* dapat menghasilkan logfile yang merekam kejadian–kejadian yang sedang di pantau oleh *Meter.*

2. *Meter*

   Meter ditempatkan di titik–titik pengukuran yang ditentukan oleh seorang administrator jaringan. Setiap meter akan merekam secara selektif aktifitas jaringan sesuai dengan konfigurasi *Manager* yang telah diarahkan. Meter juga dapat melakukan agregasi, transformasi dan proses lebih lanjut terhadap aktifitas yang direkam sebelum data disimpan atau dikirimkan kepada *Meter Reader.*

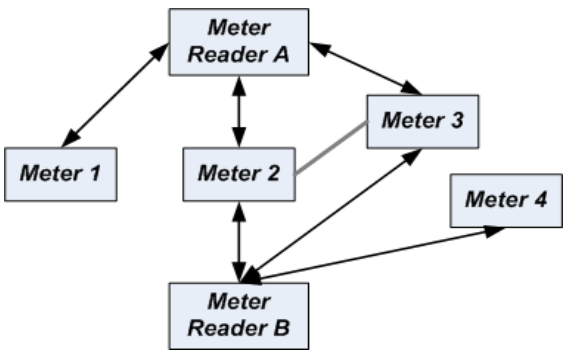
3. *Meter Reader*

   Meter Reader bertindak sebagai pengirim data-data yang diperoleh melalui *Meter* yang selanjutnya dapat diolah *ke Analysis Application*.

4. *Analysis Application*

   Analysis Application memproses data yang diterima dan selanjutnya dapat memberikan informasi dan reporting untuk keperluan manajemen jaringan. Informasi meliputi : *Traffic Flow Matrices, Flow Rate Frequency Distributions, Usage Data*

Pengoperasian sistem pengukuran lalu lintas secara keseluruhan adalah yang terbaik dipahami dengan mempertimbangkan interaksi antara komponen-nya. Ini dijelaskan sebagai berikut : Setiap *Meter* dapat dibaca oleh beberapa *Meter Reader*, seperti ditunjuk di gambar 8. *Meter 1* dibaca oleh *Meter Reader A* dan *Meter 4* dibaca oleh *Meter Reader B. Meter 1* dan *Meter 4* tidak memiliki redundansi sehingga jika *Meter* tidak berfungsi, data untuk segmen jaringan tertentu akan hilang. *Meter 2* dan *Meter 3* melakukan pengukuran lalu lintas data pada segmen jaringan yang sama. *Meter 2* dan *Meter 3* dibaca oleh *Meter Reader A* dan *Meter Reader B*. jika sebuah *Meter Reader* tidak berfungsi, maka *Meter Reader* yang lain tetap akan mengumpulkan data dari kedua *Meter 2* dan *Meter 3*.



Gambar 8. Interaksi antara Meter Reader dengan Meter (RFC 2722)

IX. ARSITEKTUR YANG DIUSULKAN

Dari hasil penelitian pendahuluan yang dilakukan, dapat diusulkan arsitektur *real-time system* sebagai pemantauan jaminan QoS. Adapun arsitektur tersebut adalah dengan mengambil pemodelan dasar dari RTFM *(Real Time Flow Measurement)* yang dipadukan

dengan *Network Monitoring Tools* yang umum telah digunakan oleh banyak administrator jaringan komputer, yaitu berbasis SNMP *(Simple Network Management Protocol)* dan/atau Penyadap Paket *(Sniffer packet)* dan/atau ICMP *(Internet Control Message Protocol)* dengan tambahan pembangunan aplikasi yang dibuat secara khusus untuk menjembataninya sekaligus melakukan manajemen dan pemantauan jaminan QoS pada jaringan terpasang secara *real-time system*. Sistem diterapkan baik di sisi penyedia layanan maupun pengguna layanan dengan sistem silang, artinya baik sisi penyedia maupun pengguna layanan melakukan pengukuran di meter sisi sendiri maupun meter sisi pasangannya. Melalui penerapan ini proses pembandingan analisa jaringan dapat diwujudkan guna memperoleh pemantauan yang mendekati kenyataan jaringan yang diamati.

X. KESIMPULAN

Melalui arsitektur yang diusulkan tersebut upaya pemantauan jaminan QoS berbasis *real-time system* untuk melakukan pengukuran dan pelaporan aliran paket data di jaringan berbasis pemantauan IP, yang merupakan pemantauan jaminan QoS baik *EtE QM* maupun *DM* sangat dimungkinkan diwujudkan. Hipotesis tersebut akan menjadi acuan penelitian lanjutan yaitu Kerangka Sistem Pengukuran Internet Sebagai Rekomendasi Penyedia & Pengguna Internet.

Harapan akhir permasalahan jaringan komputer global (Internet) yang semakin komplek setiap waktu dapat dijembatani, sehingga baik pihak penyedia atau pengguna layanan Internet terpuaskan.

Daftar Pustaka

[Arw02] Arwin D.W. Sumari (2002), "Teknologi Real-Time: Konsep dan Aplikasi".

[Bam10] Bambang Sridadi (2010), "System Waktu Nyata, Informatika Bandung

[Bud02] Budi Rahardjo (2002), '*Network Monitoring Security*', INDOCISC.COM

[BYJ00] B. Y. Jiang, C. Tham and C. Ko, (2000), "Challenges and Approaches in Providing QoS Monitoring", Int. J. Network Mgmt 2000.

[KiG09] Ki Grinsing (2009), "Masalah Jaringan", SYSNETA.COM.

[Onn01] Onno W., Purbo (2001. TCP/IP, Elex Media Komputindo, Jakarta.

[Roh08] Rohit Joshi, Chen-Khong Tham (2008). "Integrated Quality of Service and Network Management ", Deptment of Electrical Engineering, National University of Singapore

[Rtf97] __, 1997," The RTFM Architecture", The IETF RTFM Working Group

[Rfc99] __,1999,"RFC 2722 - Traffic Flow Measurement: Architecture", *Network Working Group*

[Sya09] Syamsul Akbar Syarif (2009),"Real Time System",ITI.

[Tau01] Taufan, Reza (2001), "Manajemen Jaringan TCP/IP", Elex Media Komputindokarta.

[Tut09] Tutun Juhana (2009), "Manajemen Jaringan", Makalah STEI-ITB.

[Yoa05] Yoanes Bandung, Suhardi, Armein Z.R. Langi (2005),"Metoda Real Time Flow Feasurement (RTFM) untuk monitoring QoS di jaringan NGN ", Kelompok Keahlian Sistem Informasi, Sekolah Teknik Elektro dan Informatika ITB