



UNIVERSITAS INDONESIA

**PENGUKURAN PARAMETER KUALITAS LAYANAN (QoS)
TRAFIK *VIDEO STREAMING* PADA JARINGAN IP
BERBASIS *SWITCH LAYER 2***

SKRIPSI

**SLAMET SUDIARJO
0706199930**

**FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
UNIVERSITAS INDONESIA
JANUARI 2010**



UNIVERSITAS INDONESIA

**PENGUKURAN PARAMETER KUALITAS LAYANAN (QoS)
TRAFIK *VIDEO STREAMING* PADA JARINGAN IP
BERBASIS *SWITCH LAYER 2***

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana
Teknik

**SLAMET SUDIARJO
0706199930**

**FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
UNIVERSITAS INDONESIA
JANUARI 2010**

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar

Nama : Slamet Sudiarjo
NPM : 0706199930
Tanda Tangan :
Tanggal : 4 Januari 2010



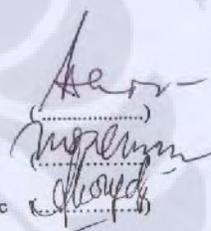
HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : Slamet Sudiarjo
NPM : 0706199930
Program Studi : Teknik Elektro
Judul Tugas Akhir : PENGUKURAN PARAMETER KUALITAS
LAYANAN (QoS) TRAFIK *VIDEO STREAMING*
PADA JARINGAN IP BERBASIS *SWITCH LAYER*
2

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Prof. Dr. Ir Bagio Budiardjo, MSc
Penguji : Muhammad Salman ST., MIT
Penguji : Prima Dewi Purnamasari ST., MT., MSc



Ditetapkan di : Universitas Indonesia
Tanggal : 4 Januari 2010

Universitas Indonesia

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Tugas Akhir ini. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

- (1) Prof. Dr. Ir. Bagio Budiardjo, M.Sc selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan Tugas Akhir ini;
- (2) PPSI dan GDLN yang telah menjadi laboratorium yang bersifat *free of charge* buat saya;
- (3) Orang tua dan keluarga saya yang secara total memberikan dukungan moral serta doa; dan
- (4) Sahabat yang telah banyak membantu saya dalam menyelesaikan Tugas Akhir ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Tugas Akhir ini membawa manfaat bagi pengembangan ilmu.

Depok, 4 Januari 2010

Penulis

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Slamet Sudiarjo
NPM : 0706199930
Program Studi : Teknik Elektro
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

**PENGUKURAN PARAMETER KUALITAS LAYANAN (QoS)
TRAFIK VIDEO STREAMING PADA JARINGAN IP
BERBASIS SWITCH LAYER 2**

Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Universitas Indonesia
Pada tanggal : 4 Januari 2010
Yang menyatakan

(Slamet Sudiarjo)

ABSTRAK

Nama : Slamet Sudiarjo
Program Studi : Teknik Elektro
Judul : Pengukuran Parameter Kualitas Layanan (QoS) Trafik Video Streaming pada jaringan IP berbasis *switch layer 2*

Switch layer 2 dapat mengklasifikasikan *incoming packet* pada port *input* berdasarkan *access-list* yang didefinisikan untuk menandai paket. Ketika paket datang ke port *switch layer-2*, paket yang sesuai dengan *attachment access-list* akan diberikan nilai berdasarkan konfigurasi sehingga paket yang kelasnya lebih tinggi akan didahulukan pada saat *traffic* jaringan telah memenuhi *bandwidth* yang tersedia. Dalam Tugas Akhir ini digunakan tiga jenis aplikasi untuk uji coba, yaitu *Video Conference* dengan UDP, Web akses dengan HTTP, *Packet Generator* dengan TCP dan UDP. Dilakukan uji coba pengkelasan masing-masing aplikasi sehingga didapatkan kondisi terbaik pada saat *bandwidth* maksimal, 10 Mbps. Pada saat tersebut *video conference* berada pada kelas 3, *website* pada kelas 1, dan *packet generator* pada kelas 2, dimana kelas dengan nilai terbesar memiliki prioritas tertinggi. Untuk melihat berapa *bandwidth* yang terpakai pada jaringan digunakan “Cacti” dan untuk mengambil jalannya paket pada jaringan digunakan “Wireshark”. Dari hasil pengujian diperoleh Delay sebesar 7086 ms, Jitter sebesar 7400,86 ms untuk *video protocol* dan 2963,02 ms untuk *audio protocol* dan Packet Loss sebesar 4000 paket atau 22,22 %. Kondisi ini terjadi pada saat aplikasi *video conference* diset pada kelas 1, aplikasi *website* pada kelas 3 dan *Packet Generator* pada kelas 5

Kata kunci: Video Conference, Switch Layer 2, Bandwidth, Jitter, Packet Loss, Wireshark, Cacti

ABSTRACT

Name : Slamet Sudiarjo
Major : Electrical Engineering
Title : The Measurement of QoS Parameter of Video Streaming Traffic
on IP network with Second Layer Switch

Layer 2 switch can classify the incoming packet based on the input port access-list is defined to mark the packet. When the packet comes into port layer-2 switch, which according to packet access-list attachment will be given based on the value of the configuration so that packets a higher class will take precedence at the network traffic meets the available bandwidth. This Final Project using three types of application, namely Video Conference with UDP, Web access with HTTP, Packet Generator with TCP and UDP. At this time the trial will be conducted classify each packet so that the best conditions obtained at maximum bandwidth, 10 Mbps. That are at the time of video conferencing is in class 3, Web site in class 1, and packet generator in class 2. To see how much bandwidth is used on the network, used "Cacti" as bandwidth monitoring and to take the course package used "Wireshark" on the network. According to the trial, take place Delay about 7086 ms, Jitter about 7400.86 ms for video protocol and 2963,02 ms for audio protocol, and number of Packet loss about 4000 packets from 18000 or 22.22 %. The condition happened when video conference application in class 1, website in class 3, and Packet Generator in class 5.

Keywords: *Video Conference, Layer-2 Switch, Bandwidth, Jitter, Packet Loss, Wireshark, Cacti*

DAFTAR ISI

KATA PENGANTAR	vi
ABSTRACT	viii
ABSTRAK	ix
DAFTAR ISI	x
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv
1. PENDAHULUAN	1
Latar Belakang.....	1
Tujuan Penulisan.....	2
Batasan Masalah.....	2
Metodologi Penyelesaian Masalah.....	2
Sistematika Penulisan.....	3
2. LANDASAN TEORI	4
Konsep Jaringan Komputer.....	4
Elemen Dasar Jaringan Komputer.....	4
Konsep TCP/IP.....	6
Monitoring Jaringan menggunakan CACTI.....	13
<i>Video Conference</i>	15
<i>Quality of Service</i>	23
3. PERENCANAAN DAN UJI COBA	28
Pendahuluan.....	28
Topologi Jaringan.....	28
Perangkat Pendukung Infrastruktur.....	29
Instalasi Infrastruktur.....	32
Pengukuran <i>Quality of Service (QoS)</i>	35
4. HASIL PENGUKURAN DAN ANALISIS DATA	39
Pengamatan Paket.....	39
Pengukuran <i>Delay</i>	42
Pengukuran <i>Jitter</i>	44

Pengukuran <i>Bandwidth</i>	45
Pengukuran <i>Throughput</i>	46
5. KESIMPULAN	48
DAFTAR REFERENSI	49
LAMPIRAN 1	
LAMPIRAN 2	



DAFTAR GAMBAR

Gambar 2.1	Model Protokol TCP/IP.....	8
Gambar 2.2	Pergerakan Data pada Layer TCP/IP.....	9
Gambar 2.3	Komponen RTP Header.....	12
Gambar 2.4	Rekomendasi <i>CCITT NO. H.261 Codec</i>	20
Gambar 2.5	Anggota protokol H.323.....	23
Gambar 2.6	Siklus Quality of Service pada cisco switch	24
Gambar 2.7	<i>Field of IP Precedence</i>	25
Gambar 3.1	Topologi jaringan Video Conference	28
Gambar 3.2	<i>Interface Packet Generator</i>	30
Gambar 3.3	<i>Monitoring port 24 cisco catalyst</i>	31
Gambar 3.4	<i>Interface Wireshark</i>	32
Gambar 3.5	Memulai install NetMeeting	33
Gambar 3.6	Menjelaskan fungsi dari NetMeeting	33
Gambar 3.7	Interface NetMeeting	34
Gambar 3.8	Setting Packet Generator Client.....	36
Gambar 3.9	Langkah menjalankan Wireshark	36
Gambar 3.10	Memanggil IP endpoint.....	37
Gambar 4.1	<i>Field Differentiated Services</i>	39
Gambar 4.2	<i>Traffic flow</i> Uji coba.....	40
Gambar 4.3	Grafik perhitungan <i>paket loss</i>	41
Gambar 4.4	<i>Class selector</i> pada interface wireshark	42
Gambar 4.5	Grafik Hasil Perhitungan Delay.....	43
Gambar 4.6	Grafik Mean Jitter pada endpoint pertama.....	44
Gambar 4.7	Grafik Mean Jitter pada endpoint kedua....	44
Gambar 4.8	Traffic tiga aplikasi pada port fast ethernet switch catalyst	45
Gambar 4.9	Traffic tiga aplikasi pada port 10 Mbps switch catalyst	46
Gambar 4.10	Grafik <i>throughput</i> pada <i>endpoint</i> pertama	47
Gambar 4.11	Grafik <i>Throughput</i> pada <i>endpoint</i> kedua	47

DAFTAR TABEL

Tabel 2.1	Kompresi Suara	16
Tabel 2.2	Kompresi <i>Bandwidth</i>	19
Tabel 2.3	<i>ITU-T Multimedia Conferencing Standar (Basic Modes)</i>	21



BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Video conference berbasis IP merupakan sebuah layanan telekomunikasi yang mampu melewatkan sinyal suara dan sinyal gambar dalam bentuk paket IP. Aplikasi *video conference* membutuhkan *bandwidth* yang cukup lebar agar memenuhi kualitas yang bagus. Apabila paket gambar atau suara yang melewati sebuah jaringan mengalami *delay*, *jitter*, dan juga *packet loss* maka kualitas dari aplikasi video conference akan menurun. Apabila *bandwidth* pada jaringan tidak bisa memenuhi besarnya *traffic* yang melewati, maka terjadi *congestion* dan *delay* pada sebuah perangkat jaringan yang dilewati *traffic* tersebut. Sedangkan *packet loss* terjadi apabila paket yang melalui jaringan tidak dapat sampai pada node perangkat tujuan dan juga disebabkan apabila *time to live* pada saat *buffering* di sebuah node jaringan telah habis.

Untuk mengatasi masalah terbatasnya bandwidth pada sebuah jaringan bisa dilakukan klasifikasi aplikasi yang melewati sebuah jaringan atau sering disebut *Quality of Service (QoS)*. Setiap perangkat jaringan mempunyai cara konfigurasi yang berbeda-beda dalam implementasi *Quality of Service*. Pada tugas akhir ini akan dibahas implementasi *Quality of Service* pada perangkat jaringan cisco switch Layer 2 dengan tipe 2950. Switch Layer 2 dengan dukungan software Cisco *Enhance Image* mampu melakukan *classification*, *marking*, dan *Policing* paket-paket yang melalui port switch layer 2. Klasifikasi dan prioritas input traffic pada Cisco Switch Layer 2 berdasarkan nilai *DiffServe Code Point (DSCP)* yang nilainya dipetakan dengan nilai *Class of Service (CoS)*, sehingga paket yang sudah ditandai akan lebih diprioritaskan. Dengan implementasi *Quality of Service* pada layer 2 switch, maka kualitas aplikasi video conference diharapkan akan lebih stabil dan bagus walaupun bandwidth yang tersedia pada jaringan tidak memenuhi (penuh).

1.2 TUJUAN PENULISAN

Tujuan penulisan Tugas Akhir ini adalah melakukan pengukuran *bandwidth, packet loss, delay, jitter, dan throughput* paket *video conference* yang dibebani berbagai aplikasi sehingga mendapatkan kondisi terbaik.

1.3 BATASAN MASALAH

Pokok bahasan pada Tugas Akhir ini adalah pengukuran parameter *Quality of Service (QoS)* pada jaringan antar switch layer 2 dengan aplikasi *video conference, website, dan packet generator*.

1.4 METODOLOGI PENYELESAIAN MASALAH

Metodologi pembahasan yang digunakan dalam penulisan Tugas Akhir ini adalah:

1.4.1 Studi pustaka:

a) Pencarian referensi

Mencari referensi yang berhubungan dengan jaringan komputer, dasar-dasar dan konfigurasi switch, perangkat video conference, protokol video conference, dan parameter-parameter *Quality of Service (QoS)*.

b) Pendalaman materi

Mempelajari dan memahami materi yang berhubungan dengan Tugas Akhir ini, seperti melakukan observasi lewat internet untuk mencari pengetahuan tambahan yang tidak terdapat pada buku-buku literature serta melakukan konsultasi kepada Pembimbing Tugas Akhir maupun diskusi dengan teman-teman.

1.4.2 Perancangan dan pengukuran.

Perancangan Jaringan dengan menggunakan konsep analisis dan desain sehingga dapat dilakukan secara terstruktur.

1.4.3 Penyusunan laporan Tugas Akhir dan kesimpulan akhir.

1.5 SISTEMATIKA PENULISAN

Sistematika penulisan pada Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang, tujuan penulisan, pembatasan masalah dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan menjelaskan tentang teori pendukung dari permasalahan *Quality of Service* di dalam jaringan komputer dengan *video conferencing* sebagai aplikasinya.

BAB III PERANCANGAN SISTEM DAN UJI COBA

Bab ini membahas tentang perancangan dan uji coba konfigurasi *Quality of Service* (QoS) di perangkat jaringan dan perangkat *video conference*.

BAB IV HASIL UJI COBA DAN ANALISIS DATA

Bab ini menjelaskan tabel dan grafik data hasil percobaan

BAB V KESIMPULAN

Berisi kesimpulan akhir dan saran terhadap pengembangan dari penelitian Tugas Akhir ini selanjutnya

BAB 2

JARINGAN BERBASIS TCP/IP DAN KUALITAS LAYANAN (QoS)

2.1 Konsep Jaringan Komputer

Jaringan Komputer adalah sekelompok komputer individu yang saling berhubungan antara satu sama lain menggunakan protokol komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, hardisk, dan lain sebagainya. Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komputer yang berada diberbagai lokasi yang terdiri lebih dari satu komputer yang saling berhubungan.

Pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat. Setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ketempat lainnya. Sehingga dapat terbentuk data yang terintegrasi, dengan demikian memudahkan pemakai untuk memperoleh dan mengolah informasi setiap saat.

Dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer dapat memudahkan pemakai dalam merawat hardisk dan peralatan lainnya, misalnya untuk memberikan perlindungan terhadap serangan virus maka pemakai cukup memusatkan perhatian pada hardisk yang ada di komputer pusat.

Dengan adanya pemakaian sumber daya secara bersama-sama, maka pemakai bisa mendapatkan hasil dengan maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera langsung diketahui oleh setiap pemakai.[1]

2.2 Elemen Dasar Jaringan

Jaringan komputer tersusun dari beberapa elemen dasar yang meliputi komponen hardware dan software, yaitu :

1. Komponen Fisik :
 - a. *Personal Computer* (PC) :

Tipe personal komputer yang digunakan di dalam jaringan akan sangat menentukan unjuk kerja dari jaringan tersebut. Komputer dengan unjuk kerja tinggi akan mampu mengirim dan mengakses data dalam jaringan dengan cepat. Di dalam jaringan tipe Client-Server, komputer yang difungsikan sebagai server mutlak harus memiliki unjuk kerja yang lebih tinggi dibandingkan komputer-komputer lain sebagai workstation-nya, karena server akan bertugas menyediakan fasilitas dan mengelola operasional jaringan tersebut.

b. *Router*

Router adalah sebuah device yang berfungsi untuk meneruskan paket-paket dari sebuah network ke network yang lainnya (baik LAN ke LAN atau LAN ke WAN) sehingga host-host yang ada pada sebuah network bisa berkomunikasi dengan host-host yang ada pada network yang lain. Router menghubungkan network-network tersebut pada network layer dari model OSI, sehingga secara teknis Router adalah Layer 3 Gateway.

Router bisa berupa sebuah device yang dirancang khusus berfungsi sebagai router atau bisa juga berupa sebuah PC yang difungsikan sebagai router

c. *Switch*

Switch jaringan (atau switch untuk singkatnya) adalah sebuah alat jaringan yang melakukan *bridging transparan* (penghubung segmentasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC). Switch jaringan dapat digunakan sebagai penghubung komputer atau router pada satu area yang terbatas, switch bekerja pada lapisan data link, cara kerja switch hampir sama seperti bridge, tetapi switch memiliki sejumlah port sehingga sering dinamakan *multi-port bridge*. [2]

d. *Unshielded twisted-pair* (UTP)

Unshielded twisted-pair (UTP) adalah sebuah jenis kabel jaringan yang menggunakan bahan dasar tembaga, yang tidak dilengkapi dengan *shield* internal. UTP merupakan jenis kabel yang paling umum yang sering digunakan di dalam jaringan lokal (LAN), karena memang harganya yang

rendah, fleksibel dan kinerja yang ditunjukkannya relatif bagus. Dalam kabel UTP, terdapat insulasi satu lapis yang melindungi kabel dari ketegangan fisik atau kerusakan tapi, tidak seperti kabel *Shielded Twisted-pair* (STP), insulasi tersebut tidak melindungi kabel dari interferensi elektromagnetik.[3]

2. Komponen *Software* :

Sistem Operasi, Adapter Driver, Protokol Jaringan.

a. Sistem Operasi:

Sistem Operasi merupakan perangkat lunak yang mengatur sistem kerja dari perangkat keras sehingga dapat bekerja sesuai dengan program yang akan digunakan. Untuk Sistem operasi yang sering dipakai adalah Windows proprietary dari Microsoft dan Linux yang berbasis komunitas.

b. Adapter Driver

Adapter Driver merupakan sebuah perangkat lunak yang berfungsi mengantarkan optional peripheral sehingga dapat berinteraksi dengan sistem operasi.

c. Protokol Jaringan

Protokol jaringan adalah peraturan-peraturan yang telah disepakati bersama atau dikeluarkan oleh perusahaan jaringan sehingga dijadikan bahan untuk membangun jaringan, dan ada beberapa yang diwujudkan dalam bentuk perangkat lunak. Sebagai contoh adalah *Open Shortes Path First* (OSPF) yang digunakan sebagai protokol routing.

2.3 Konsep TCP/IP

Dalam dunia komunikasi data, protokol mengatur bagaimana sebuah komputer berkomunikasi dengan komputer lain. Dalam jaringan komputer kita dapat menggunakan banyak macam protokol tapi agar sebuah komputer dapat berkomunikasi, keduanya harus menggunakan protokol yang sama. Protokol berfungsi mirip dengan bahasa. Agar dapat berkomunikasi seseorang perlu berbicara dan mengerti bahasa yang mereka gunakan.

TCP/IP (*Transmission Control Protocol / Internet Protocol*) adalah sekumpulan protokol yang mengatur komunikasi data komputer dengan komputer yang lain maupun komputer dengan jaringan Internet. Karena menggunakan bahasa yang sama, yaitu protokol TCP/IP, perbedaan jenis komputer dan sistem operasi tidak menjadi masalah.

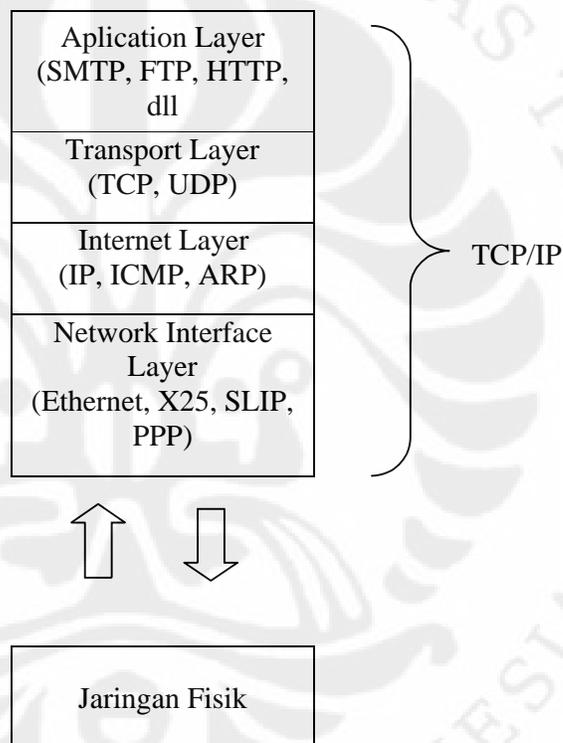
Komputer PC dengan menggunakan sistem operasi Windows dapat berkomunikasi dengan komputer Macintosh atau dengan Sun SPARC yang menjalankan Solaris. Jadi, jika sebuah komputer menggunakan protokol TCP/IP dan terhubung langsung ke Internet, maka komputer tersebut dapat berhubungan dengan komputer di belahan dunia manapun yang juga terhubung ke Internet.

Perkembangan TCP/IP yang diterima luas dan praktis menjadi standard defacto jaringan komputer berkaitan dengan ciri-ciri yang terdapat pada protokol itu sendiri :

- Protokol TCP/IP dikembangkan menggunakan standart protokol yang terbuka.
- Standart protokol TCP/IP dalam bentuk *Request For Comment* (RFC) dapat diambil oleh siapapun tanpa biaya.
- TCP/IP dikembangkan dengan tidak tergantung pada sistem operasi atau perangkat keras tertentu.
- Pengembangan TCP/IP dilakukan dengan konsensus dan tidak tergantung pada vendor tertentu.
- TCP/IP independen terhadap perangkat keras jaringan dan dapat dijalankan pada jaringan Ethernet, Token Ring, Jalur telepon dial-up, jaringan X25, dan praktis jenis media transmisi apa pun.
- Pengalamatan TCP/IP bersifat untuk dalam skala global. Dengan cara ini, komputer dapat saling terhubung walaupun jaringannya seluas internet sekarang ini.

TCP/IP bukanlah sebuah protokol tunggal, tetapi satu kesatuan protokol. TCP/IP merupakan sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada *Wide Area Network* (WAN). TCP/IP terdiri dari protokol-protokol yang bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Berkat prinsip ini, tugas masing-masing protokol menjadi jelas

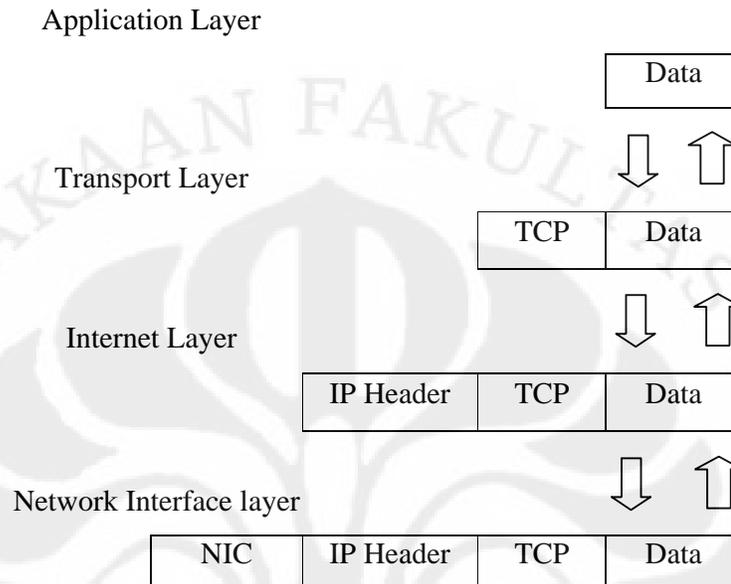
dan sederhana. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih bisa mengirim dan menerima data. Berkat penggunaan prinsip ini, TCP/IP menjadi protokol komunikasi data yang fleksibel. Protokol TCP/IP dapat diterapkan dengan mudah di setiap jenis komputer dan interface jaringan, karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu. Sekumpulan protokol TCP/IP ini dimodelkan dengan empat layer TCP/IP, sebagai mana terlihat pada gambar di bawah ini.[4]



Gambar 2.1 Model Protokol TCP/IP[4]

Jika suatu protokol menerima data dari protokol lain di layer atasnya, ia akan menambahkan informasi tambahan miliknya ke data tersebut, informasi ini memiliki fungsi yang sesuai dengan fungsi protokol tersebut. Setelah itu, data ini diteruskan lagi keprotokol pada layer dibawahnya. Hal ini yang sebaliknya terjadi jika suatu protokol menerima data dari protokol lain yang berada pada layer dibawahnya. Jika data ini dianggap valid, protokol akan melepas informasi

tambahan tersebut, untuk kemudian meneruskan data itu ke protokol lain yang berada pada layer di atasnya. Pergerakan data dalam layer TCP/IP seperti gambar dibawah ini:



Gambar 2.2 Pergerakan data dalam layer TCP/IP

TCP/IP terdiri atas empat lapis kumpulan protokol yang bertingkat.

Keempat lapisan/layer tersebut adalah :

1. Network Interface Layer

Bertanggung jawab mengirim dan menerima data ke dan dari media fisik (berupa kabel, serat optik atau gelombang radio), maka dari itu harus mampu menerjemahkan sinyal listrik menjadi digital yang dimengerti komputer.

2. Internet Layer

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol yaitu:

- IP (Internet Protokol) berfungsi untuk menyampaikan paket data ke alamat yang tepat, IP memiliki sifat sebagai unreliable (ketidakandalan: tidak menjamin datagram yang terkirim sampai tujuan), connectionless, datagram delivery service.

- ARP (Address Resolution Protokol) Protokol yang digunakan untuk menemukan alamat Hardware dari host/komputer yang terletak pada network yang sama.
- ICMP (Internet Control message protokol) Protokol yang digunakan untuk mengirimkan pesan dan melapor kegagalan pengiriman data.

3. Transport Layer

Bertanggung jawab untuk mengadakan komunikasi antara dua host/komputer, yang terdiri dari protokol TCP (Transmission Control Protokol) dan UDP (User Datagram Protokol). TCP merupakan protokol yang menyediakan service *connection oriented*, sebelum melakukan pertukaran data, dua aplikasi pengguna TCP harus melakukan pembentukann hubungan terlebih dahulu.

4. Aplication Layer

Terletak semua aplikasi yang menggunakan protokol TCP/IP.

Fungsi masing-masing layer / lapisan protokol serta aliran data pada layer TCP / IP diatas, dapat dicontohkan dengan menggunakan analogi yang sangat sederhana. Seperti analogi pengiriman surat, seperti berikut ini:

1. Pertama, kita harus menulis dahulu isi surat tersebut. Maka kita harus mengambil selembor kertas dengan ballpoint untuk mrnulis berita tersebut.
2. Setelah langkah ini terselesaikan, maka kita harus mengambil amplop surat agar terlindung dari kerusakan.
3. Maka kita harus memilih amplop yang tertutup (TCP) atau amplop yang terbuka (UDP).
4. Barulah kita menulis alamat yang dituju dengan jelas, serta nama pengirim dan alamat pengirim.
5. Maka selesailah sudah pengiriman surat tersebut dengan menitipkan surat itu pada kantor pos.

Cara kerja TCP/IP dalam satu komputer adalah sangat mirip dengan cerita diatas. Mengirimkan e-mail dll, terlebih dahulu diolah di TCP. Saat diolah TCP memberi amplop untuk melindungi data-data yang hendak dikirim, yang berupa

data tambahan (no.urut), 16 bit source port number (nama pengirim dan penerima).[4]

2.3.1 Internet Protocol (IP)

Internet Protocol didesain untuk interkoneksi sistem komunikasi komputer pada jaringan *paket switched*. Pada jaringan TCP/IP, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data. Untuk komunikasi datanya, *Internet Protokol* mengimplementasikan dua fungsi dasar yaitu *addressing* dan fragmentasi.

Salah satu hal penting IP dalam pengiriman informasi adalah metode pengalamatan pengirim dan penerima. Saat ini terdapat standar pengalamatan yang sudah digunakan yaitu IPv4 dengan alamat terdiri dari 32 bit. Jumlah alamat yang diciptakan dengan IPv4 diperkirakan tidak dapat mencukupi kebutuhan pengalamatan IP sehingga sekarang sudah tersedia sistim pengalamatan yang baru yaitu IPv6 yang menggunakan sistim pengalamatan 128 bit.[5]

2.3.2 User Datagram Protocol (UDP)

UDP yang merupakan salah satu *protocol* utama diatas IP dan merupakan *transport protocol* yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas. *Header* UDP hanya berisi empat *field* yaitu *source port*, *destination port*, *length* dan *UDP checksum* dimana fungsinya hampir sama dengan TCP, namun fasilitas *checksum* pada UDP bersifat opsional.

UDP pada *video conference* digunakan untuk mengirimkan *audio and video stream* yang dikirimkan secara terus menerus. UDP digunakan pada *video conference* karena pada pengiriman *audio and video streaming* yang berlangsung terus menerus lebih mementingkan kecepatan pengiriman data agar tiba di tujuan

tanpa memperhatikan adanya paket yang hilang walaupun mencapai 50% dari jumlah paket yang dikirimkan.

Karena UDP mampu mengirimkan data *streaming* dengan cepat, maka dalam teknologi Video Conference maupun VoIP UDP merupakan salah satu *protokol* penting yang digunakan sebagai *header* pada pengiriman data selain RTP dan IP. Untuk mengurangi jumlah paket yang hilang saat pengiriman data (karena tidak terdapat mekanisme pengiriman ulang) maka pada teknologi VoIP pengiriman data banyak dilakukan pada *private network*. [5]

2.3.3 RTP (Real-time Transport Protocol)

Protokol RTP menyediakan transfer media secara *real-time* pada jaringan paket. Protokol RTP menggunakan Protokol UDP dan *header* RTP mengandung informasi kode bit yang spesifik pada tiap paket yang dikirimkan; hal ini membantu penerima untuk melakukan antisipasi jika terjadi paket yang hilang.

RTP adalah protokol yang dibuat untuk mengkompensasi *jitter* dan *desequencing* yang terjadi pada jaringan IP. RTP dapat digunakan untuk beberapa macam data stream yang *realtime* seperti data suara dan data video. RTP berisi informasi tipe data yang di kirim, *timestamps* yang digunakan untuk pengaturan waktu suara percakapan terdengar seperti sebagaimana diucapkan, dan *sequence numbers* yang digunakan untuk pengurutan paket data dan mendeteksi adanya paket yang hilang.

0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
<u>Ver</u>	<u>P</u>	<u>X</u>	<u>CC</u>				<u>M</u>	<u>PT</u>											<u>Sequence Number</u>													
<u>Timestamp</u>																																
<u>SSRC</u>																																
<u>CSRC</u> [0..15] :::																																

Gambar 2.3 Komponen RTP header [6]

RTP didesain untuk digunakan pada *transport layer*, namun demikian RTP digunakan diatas UDP, bukan pada TCP karena TCP tidak dapat beradaptasi pada pengiriman data yang *real-time* dengan keterlambatan yang relatif kecil seperti pada pengiriman data komunikasi suara.

Dengan menggunakan UDP yang dapat mengirimkan paket IP secara *multicast*, RTP *stream* yang di bentuk oleh satu terminal dapat dikirimkan ke beberapa terminal tujuan.[6]

2.4 Monitoring Jaringan menggunakan Cacti

Cacti merupakan salah satu tools yang digunakan untuk me-monitor jaringan baik dalam skala besar maupun kecil. Seperti halnya tools monitoring jaringan yang lain, cacti mampu mem-visualisasikan bandwidth dalam jaringan yang sudah terpakai, utility dari Server, monitoring perangkat jaringan atau server yang aktif dan mati.

Cacti merupakan frontend dari RRDTool, cacti mengumpulkan informasi yang di butuhkan untuk pembuatan grafik dan menyimpan informasi tersebut menjadi data dalam database MySQL. Fronted tersebut dibuat sepenuhnya menggunakan bahasa pemrograman PHP.[7]

Selain kemampuan untuk memaintain grafik, Data Sources dan Round Robin arsip dalam database, dalam menhandel pengumpulan data. Cacti juga support SNMP (sama seperti MRTG). Ada empat komponen utama Cacti, yaitu:

2.4.1 Data Sources

Untuk menhandel pengumpulan data , dapat dibuat eksternal *script* atau *command* yang akan diperlukan untuk di pilih, cacti kemudian mengumpulkan melalui *cron job* dan menyimpan nya kedalam *database* atau *round robin archives*.

Data Sources dapat juga di buat, yang berkoresponden dengan data sebenarnya dalam grafik. Sebagai contoh yaitu apabila ingin membuat grafik ping time ke suatu host, maka harus membuat data sources memanfaatkan skrip yang

melakukan ping suatu host yang menghasilkan nilai dalam milliseconds. Setelah mendefinisikan option untuk RRDtool sebagaimana menyimpan data anda dapat mendefinisikan informasi tambahan yang dibutuhkan oleh data input. Seperti host yang akan di ping dalam hal ini. Setelah data source di buat, lalu akan di maintain setiap 5 menit secara otomatis.

2.4.2 Graphs

Setiap satu atau lebih data source di definisikan, sebuah grafik RRDtool dapat dibuat menggunakan data tersebut. Cacti memungkinkan membuat hampir setiap grafik RRDtool yang dapat di gambarkan. Menggunakan setiap standar RRDtool grafik tipe dan fungsi gabungan. Suatu area pemilihan warna , dan fungsi pengisian text otomatis juga membantu dalam pembuatan grafik agar proses pembuatan grafik lebih mudah.

Tidak hanya bisa membuat grafik RRDTool based di cacti, tetapi banyak cara untuk menampilkan grafik. Selain dengan standar “ List view “ dan “ preview mode “ yang menyerupai RRDTool frontend untuk semua , ada “tree view”, yang memungkinkan anda untuk menaruh grafik-grafik ke suatu tree yang hirarkis untuk tujuan-tujuan pengelompokan.

2.4.3 User Management

Karena banyak fungsi cacti, sebuah user management tool builtin dibuat agar dapat menambahkan para user dan memberi hak-hak untuk bagian-bagian tertentu dari cacti. Ini akan memungkinkan seseorang untuk membuat beberapa user yang dapat merubah parameter parameter grafik, sedangkan yang lain nya hanya bisa melihat grafik. Masing masing user juga dapat memaintain setingan mereka sendiri ketika login untuk melihat grafik.

2.4.4 Templating

Cacti dapat diskalakan menjadi jumlah besar source data melalui penggunaan template. Hal ini memungkinkan pembuatan sebuah grafik atau data source

template yang menggambarkan beberapa grafik atau data source yang berhubungan dengannya. Template-template host memungkinkan anda untuk menggambarkan kemampuan dari suatu host maka cacti dapat menggunakannya untuk informasi atas penambahan suatu host yang baru.[7]

2.5 Video Conference

Dalam perencanaan untuk mengimplementasikan *video conference* pada *Local Area Network* (LAN), perlu memperhitungkan kebutuhan bandwidth, karena saat pengiriman video estimasi alokasi bandwidth menjadi sangat penting karena akan memakan sebagian besar bandwidth komunikasi yang ada. Sehingga teknik-teknik untuk melakukan kompresi data menjadi sangat strategis untuk memungkinkan penghematan bandwidth komunikasi.

Sebagai gambaran sebuah kanal gambar (video) yang baik tanpa di kompresi akan mengambil bandwidth sekitar 9 Mbps, sedangkan sebuah kanal suara (audio) yang baik tanpa di kompresi akan mengambil bandwidth sekitar 64Kbps. Dari gambaran diatas dapat diasumsikan bahwa kebutuhan minimal bandwidth yang dibutuhkan untuk mengirimkan gambar dan suara adalah sebesar 9,064 Mbps, memang akan membutuhkan bandwidth yang sangat lebar. Namun dengan teknik kompresi yang ada, sebuah kanal suara dan gambar sebelum dilewatkan dalam jaringan TCP/IP akan terlebih dahulu melalui proses kompresi sehingga dapat menghemat sebuah kanal video menjadi sekitar 30Kbps dan kanal suara menjadi 6Kbps (half-duplex), artinya sebuah saluran Local Area Network (LAN) yang memiliki bandwidth sebesar 10/100 Mbps sebetulnya dapat digunakan untuk menyalurkan video dan audio sekaligus. Tentunya untuk kebutuhan konferensi yang multiuser akan dibutuhkan multi bandwidth pula, artinya minimal sekali kita harus menggunakan kanal 32-36Kbps dikalikan dengan berapa user konferensi dilakukan dalam jaringan.[8]

2.5.1 Kompresi Suara

Pada tabel terlampir daftar beberapa teknik kompresi suara yang sering digunakan dengan beberapa parameter yang mencerminkan kinerja dari teknik kompresi suara tersebut.

Tabel 2.1 Kompresi Suara[9]

Name	standardized by	description	bit rate (kb/s)	sampling rate (kHz)
(ADPCM) DVI	Intel, <u>IMA</u>	ADPCM	32	8
G.711	<u>ITU-T</u>	Pulse code modulation (PCM)	64	8
G.721	<u>ITU-T</u>	Adaptive differential pulse code modulation (ADPCM)	32	8
G.722	<u>ITU-T</u>	7 kHz audio-coding within 64 kbit/s	64	16
G.722.1	<u>ITU-T</u>	Coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss	24/32	16
G.723	<u>ITU-T</u>	Extensions of Recommendation G.721 adaptive differential pulse code modulation	24/40	8

		to 24 and 40 kbit/s for digital circuit multiplication equipment application		
G.723.1	<u>ITU-T</u>	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s	5.6/6.3	8
G.726	<u>ITU-T</u>	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)	16/24/32/40	8
G.727	<u>ITU-T</u>	5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM)	var.	?
G.728	<u>ITU-T</u>	Coding of speech at 16 kbit/s using low-delay code excited linear prediction	16	8

G.729	<u>ITU-T</u>	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)	8	8
GSM 06.10	ETSI	Regular Pulse Excitation Long Term Predictor (RPE-LTP)	13	8

2.5.2 Kompresi Video

Pada teknik kompresi video ada dua buah standar yang umum digunakan, dalam pengiriman video melalui saluran komunikasi yang sempit, yaitu:

- H.261 – biasanya menggunakan kanal ISDN dengan kecepatan $p \times 64\text{Kbps}$, dimana p adalah 1, 2, 3, ..., 30.
- H.263 – di arahkan untuk mengirimkan gambar video berkecepatan rendah mulai dari 20-30Kbps ke atas.
- H.264, atau sering juga disebut MPEG-4/AVC. MPEG-4 AVC hanya memiliki file size seperempat dari video yang dibuat memakai MPEG-2

Video yang cukup baik biasanya dikirim dengan kecepatan frame per second (fps) sekitar 30 fps. Jika dikirimkan tanpa kompresi, sebuah video dengan 30 fps akan mengambil bandwidth kira-kira 9Mbps, amat sangat besar untuk ukuran kanal komunikasi data. Untuk memberikan gambaran bagaimana upaya untuk penghematan bandwidth dan rasio kompresi yang dibutuhkan, ada baiknya kita perhatikan tabel terlampir.

Tabel 2.2 Kompresi Bandwidth [10]

Keterangan	Rata-rata PSNR (dB)	Bitrate (Kbit/s)	Rasio Kompresi
Orisinal, 30 fps	-	9124	1:1
10fps, 20Kbps	38.51	22.81	133:1
10fps, 50Kbps	41.75	56.70	54:1
10fps, 100Kbps	43.98	112.09	27.1
10fps, 500Kbps	48.38	505.61	6:1

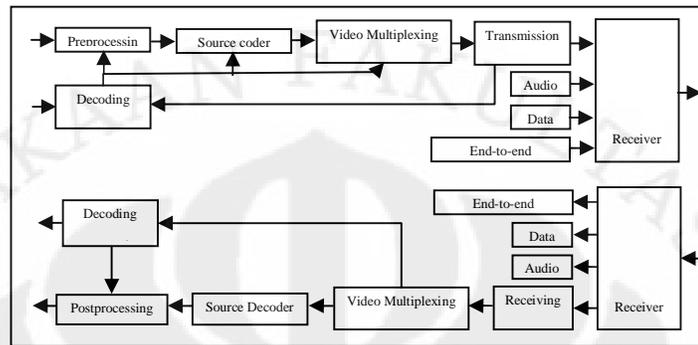
Tampak pada *tabel 2.3*, sebuah pengiriman video yang asli (tidak di kompres) dengan kecepatan 30 fps akan memakan bandwidth 9Mbps. Dalam pengiriman video untuk konferensi video melalui LAN, biasanya kita mengurangi jumlah frame yang dikirim, misalnya menjadi 10 fps. Beberapa teknik kompresi digunakan mulai dari yang paling kecil hasilnya yaitu 133:1 sampai dengan yang akan membutuhkan banyak bandwidth (500Kbps) dengan rasio kompresi 6:1. Terlihat bahwa video 10 fps hasil kompresi 133:1 dapat dikirimkan dalam kanal 23Kbps dengan rata-rata Signal To Noise Ratio 38.51dB, Tentunya jika kita ingin memperoleh kualitas yang lebih baik, PSNR yang lebih baik, kompresi dapat dikurangi hingga rasio 6:1 atau lebih rendah lagi.[10]

2.5.3 Coding dan Decoding

Salah satu komponen yang terpenting dalam video conference adalah peralatan codec (coder dan decoder), codec menggunakan teknik penyamplingan sinyal analog untuk dirubah menjadi sinyal digital lalu mereduksi lebar pita sinyal sesuai dengan kebutuhan. Algoritma sebagai proses pengkodean sinyal-sinyal informasi sehingga lebar pita sinyal tersebut dapat direduksi, dipakai pada alat codec ini untuk pengkompresan data yang telah didapat dari hasil sampling.

Pada dasarnya perencanaan kecepatan data keluaran dari codec ini dapat disesuaikan dengan kebutuhan, akan tetapi ada satu rekomendasi dari badan internasional CCITT (The Internasional Telegraph and Telephone Consultative

Commite) No. H.261 keluaran tahun 1990 yang memberikan saran bagi para perekayasa sistem untuk membuat codec video bagi pelayanan audiovisual pada kecepatan $p \times 64$ kbps dengan p bilangan bulat berkisar antara 1 – 30, yang mana rekomendasi ini akan diterangkan secara terperinci pada bagian berikut :



Gambar 2.4 Rekomendasi CCITT NO. H.261 Codec[11]

♦ Rekomendasi H.261 dari CCITT :

Rekomendasi ini menggambarkan metode coding dan decoding untuk gambar bergerak bagi pelayanan audiovisual dengan kecepatan $p \times 64$ kbps, dengan $p \times$ bilangan asli berkisar antara 1-30 dan umumnya digunakan untuk video dengan bit rate antara 40 kbps dan 2 Mbps. Blok diagram codec yang direkomendasikan adalah seperti yang digambarkan pada gambar berikut :

2.5.4 Protokol pendukung Video Conference

Pada table dibawah ini adalah standarisasi yang dikeluarkan oleh ITU-T untuk aplikasi kontrol audio, video dan multiplex pada jaringan yang mendukung standard system komunikasi video dan audio secara realtime.

Tabel 2.3 ITU-T Multimedia Conferencing Standar (Basic Modes)[11]

Standar	Network	Video	Audio	Multiplex	Control
H.320(1990)	ISDN	H.261	G.711	H.221	H.242
H.321(1995)	ATM/BISDN	Adapts H.320 to ATM/B-ISDN network			
H.322(1995)	IsoEthernet	Adapts H.320 to IsoEthernet Network			
H.323(1996)	LANs/internet	H.261	G.711	H.225.0	H.245
H.324(1995)	PSTN	H.263	G.723.1	H.223	H.245
H.310(1996)	ATM/BISDN	H.262	MPEG-1	H.222	H.245

Untuk standard H.320, H.321, dan H.322 pada dasarnya hanya mendukung komunikasi dua jalur video dan audio, dalam perkembangannya membolehkan komunikasi *multipoint* (terdapat dua atau lebih yang membentuk sebuah konferensi group virtual). Dari masing-masing standard diatas menjamin interoperability ketika digunakan dan bertemu dari network yang berbeda dengan menggunakan sebuah kontrol protocol.

Sistem atau protocol ini masuk kedalam dua generasi H.320, H321 dan H.322 adalah standar generasi pertama, didasarkan pada H.320 untuk jaringan ISDN diakui pada tahun 1990. Khusus H.321 dan H.322 diadaptasikan dari terminal H.320 untuk kegunaan pada ATM dan ISOEthernet network. Selanjutnya H.323, H.324, dan H.310 adalah generasi kedua standar protokol H, yang diakui pada tahun 1995 dan 1996.

Berdasarkan pengalaman aplikasi dilapangan dengan menggunakan H.320 pernah terjadi permasalahan ketika bertemu dengan network lain yang menggunakan protokol berbeda, untuk menghindari masalah tersebut telah

ditemukan sebuah protokol kontrol yang mendukung *interoperability* dengan menggunakan H.245, kemudian untuk standarisasi bersama kodenya menjadi H.324, yang mana seperti H.320 diperuntukkan untuk laju bit rendah. Selanjutnya H.320 mengalami perkembangan standarisasi termasuk menjadi H.323/H.324.

2.5.5 H.323 untuk Video Conference

Protokol H.323 yang terbaru versi 4 dikeluarkan pada 17 November 2000 dan menjadi protokol multipoin yang paling banyak dipergunakan, dalam perkembangannya H.323 mengalami peningkatan yang meliputi keandalan, skalabilitas, dan fleksibilitas. Menjadi Interface gateway yang berfungsi sebagai MCU (Multi Control Unit). H.323 telah menjadi protokol yang handal untuk aplikasi konferensi video, audio dan data pada jaringan TCP/IP.

H.323 memiliki mekanisme yang umum untuk menyediakan sistem multipoin audio dan video untuk aplikasi video conference, H.323 juga menyediakan point-to-point video conference. Sehingga protokol H.323 digunakan sebagai pusat pengendali komunikasi (MCU) yang terjadi saat client-client dalam jaringan melakukan komunikasi audio dan video realtime antar client dalam jaringan lokal atau internet. Dalam aplikasinya pada operating sistem Windows hanya protokol H.323 klien yang bisa mendukung Microsoft Netmeeting® untuk conference dengan menjadikannya H.323 sebagai MCU-nya yang berbasis software.[11]

H.323 merupakan terminal yang mendukung protokol H.245 yang berfungsi untuk mengendalikan pemakaian saluran dalam jaringan, protokol Q.931 untuk susunan panggilan dan memberi sinyal, serta protokol RAS (Registration/Admission/Status) yang berfungsi untuk berkomunikasi dengan Gatekeeper dan protokol RTP/RTCP yang berfungsi untuk mengatur urutan transmisi paket audio dan video. H.323 memiliki beberapa anggota protokol yang terdiri dari:

Audio applications	Video applications	Terminal control and management				Data Applications
G.711 G.722 G.723.1 G.728 G.729	H.261 H.263	RTCP	H.225.0 Terminal to Gateway signalling (RAS)	H.225.0 Call signalling	H.245 Control channel	T.124
RTP						T.125
Unreliable Transport (UDP)				Reliable Transport (TCP)		T.123
Network Layer (IP)						
Link Layer (IEEE 802.3)						
Physical Layer (IEEE 802.3)						

Gambar 2.5 Anggota protokol H.323[11]

2.6 Quality of Service (QoS)

Quality of Service (QoS) merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan melalui berbagai teknologi. Pada dasarnya, QoS memungkinkan untuk memberikan pelayanan yang lebih baik aliran (aplikasi) tertentu. Hal ini dilakukan baik dengan meningkatkan prioritas aliran atau membatasi prioritas aliran lain. Ada banyak cara dalam implementasi QoS, hal ini sesuai dengan kebutuhan jaringan dan perangkat yang digunakan. Analogi sederhana berasal dari kebutuhan untuk mengencangkan baut, jika mengencangkan baut dengan tang atau dengan kunci pas. Keduanya sama-sama efektif, tetapi ini adalah alat yang berbeda. Ini adalah sama dengan alat QoS. Akan ada penemuan hasil yang dapat dicapai dengan menggunakan alat QoS yang berbeda. Mana yang akan digunakan tergantung pada lalu lintas. Konsep dasar QoS terbagi atas 3 hal:[12]

1. Identification and Marking

Untuk memberikan layanan istimewa pada jenis lalu lintas, pertamakali paket harus diidentifikasi. Kedua, paket mungkin atau mungkin tidak akan ditandai. Kedua tugas membuat klasifikasi. Ketika *paket* diidentifikasi tetapi tidak ditandai, klasifikasi dikatakan *per-hop basis*. Hal ini terjadi ketika klasifikasi berkenaan hanya untuk perangkat yang aktif, tidak diteruskan ke perangkat berikutnya. Hal ini terjadi pada *Priority Queuing* (PQ) dan *Custom Queuing* (CQ). Ketika paket

ditandai untuk penggunaan ke perangkat berikutnya, maka klasifikasi baru dilakukan.

2. *Queuing and Scheduling*

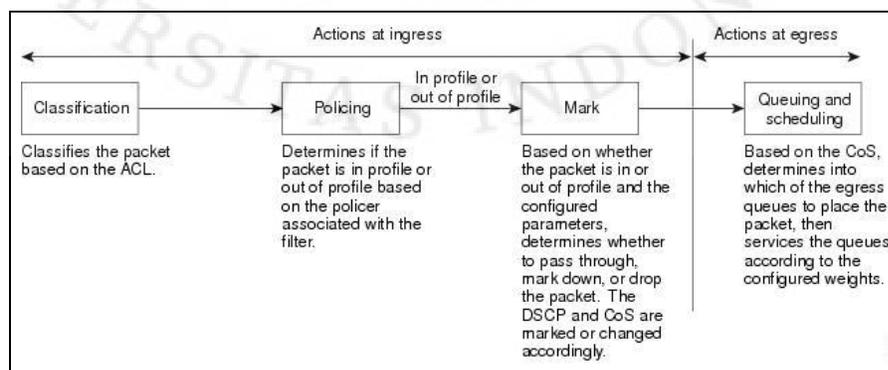
Karena ukuran antrian yang tak terhingga, mereka dapat mengisi dan melimpah. Ketika antrian penuh, paket tambahan tidak bisa masuk ke antrian dan akan dikeluarkan. Ini adalah ekor drop. Masalah dengan ekor tetes adalah bahwa router tidak dapat mencegah paket ini dari yang dijatuhkan (bahkan jika itu adalah paket prioritas tinggi). Jadi, suatu mekanisme yang diperlukan untuk melakukan dua hal:

- a. Memastikan untuk tidak terjadi antrian penuh, sehingga ada ruang untuk paket prioritas tinggi
- b. Membiarkan semacam kriteria untuk men-*drop* paket-paket yang lebih rendah sebelum men-*drop* prioritas-prioritas paket yang lebih tinggi

3. *Policy and Management*

Manajemen QoS membantu untuk menetapkan dan mengevaluasi kebijakan QoS. Metodologi yang umum mencakup langkah-langkah berikut:

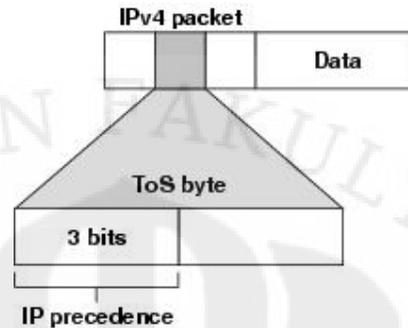
- a. Mendasari dengan perangkat jaringan seperti RMON probe. Ini membantu dalam menentukan karakteristik lalu lintas jaringan. Selain itu, aplikasi yang ditargetkan untuk QoS harus berjajar dasar (biasanya dalam hal waktu respon).
- b. Menyebarkan teknik QoS ketika karakteristik lalu lintas telah didapatkan dan sebuah aplikasi telah diketahui untuk meningkatkan QoS.
- c. Mengevaluasi hasil-hasil dengan menguji respon dari aplikasi yang ditargetkan untuk melihat apakah tujuan QoS telah dicapai.[13]



Gambar 2.6 Siklus Quality of Service pada cisco switch[13]

2.6.1 IP Precedence dan Differentiated QoS

IP Precedence memanfaatkan 3 bit Precedence pada header IPv4's Type of Service (ToS) untuk menentukan layanan kelas untuk setiap paket, seperti ditunjukkan pada Gambar berikut



Gambar 2.7 field of IP Precedence[13]

3 bit MSB (yang berhubungan dengan pengaturan biner 32, 64, dan 128) dari Jenis field dalam header IP merupakan bit yang digunakan untuk IP Precedence. Bit ini digunakan untuk memberikan prioritas 0-7 untuk paket IP.

2.6.2 Aspek kuantitatif Kualitas Layanan (QoS)

Jika dilihat dari ketersediaan suatu jaringan, terdapat karakteristik kuantitatif yang dapat dikontrol untuk menyediakan suatu layanan dengan kualitas tertentu. Karakteristik layanan tersebut adalah:

1. Delay

Delay oleh trafik layanan (paket) adalah aspek yang sangat penting suatu kualitas layanan. Berbagai aspek delay mempunyai dampak yang berbeda-beda terhadap layanan yang berbeda pula, seperti: end-to-end delay dan variasi delay atau jitter.

Aplikasi real-time interaktif, misalnya komunikasi suara, sangat sensitif terhadap end-to-end delay dan jitter. Delay yang panjang akan mengurangi interaktifitas komunikasi.

Aplikasi real-time non-interaktif, misalnya broadcast satu arah, kurang dipengaruhi oleh end-to-end delay tetapi sangat dipengaruhi oleh jitter.

Aplikasi non real-time biasanya tidak sensitif terhadap delay.

Terdapat beberapa komponen end-to-end delay :

- Delay transmisi: waktu yang dibutuhkan untuk meletakkan seluruh bit dari suatu paket ke dalam link.
- Delay propagasi: waktu yang dibutuhkan suatu bit untuk melewati suatu link (biasanya dalam kecepatan cahaya).
- Delay proses: waktu yang dibutuhkan untuk memproses suatu paket dalam suatu elemen jaringan (mis: merutekan paket pada output port).
- Delay antrian: waktu dimana suatu paket harus menunggu dalam antrian sebelum suatu paket dijadwalkan untuk ditransmisikan.

2. *Throughput*

Aspek utama throughput yaitu berkisar pada ketersediaan bandwidth yang cukup untuk suatu aplikasi. Hal ini menentukan besarnya trafik yang dapat diperoleh aplikasi saat melewati jaringan. Aspek penting lainnya adalah error (pada umumnya berhubungan dengan link error rate) dan losses (pada umumnya berhubungan dengan kapasitas buffer).

Aplikasi tertentu dapat mengurangi laju trafiknya sebagai respon terhadap indikasi throughput yang rendah (mis: mengurangi fidelity dari skema pengkodean). Aplikasi ini disebut dengan aplikasi “rate adaptive”.

Throughput tergantung pada faktor-faktor berikut ini:

- karakteristik link : bandwidth, error rate.
- karakteristik node : kapasitas buffer, daya pemrosesan.

Sebagaimana terlihat pada penjelasan tersebut, sejumlah karakteristik dari elemen jaringan yang bervariasi, seperti terminal/host, link, dan switch/router, sangat menentukan quality of service apa yang akan disediakan untuk suatu aplikasi, dalam hubungannya dengan delay dan throughput.

2.6.3 Aspek Pemenuhan *Quality of Service*

Terdapat dua mekanisme dasar dalam penyediaan *quality of service* yang memadai yang didasarkan pada nilai delay dan throughput, yaitu:

- Kapasitas yang sangat besar
- Traffic engineering

Dengan kapasitas yang sangat besar diasumsikan bahwa terdapat kapasitas yang cukup tersedia di dalam jaringan yang tidak memerlukan penyediaan mekanisme diluar itu untuk menjamin quality of service. Hal-hal berikut yang harus mencukupi sehingga dapat memenuhi syarat diatas yaitu: link dengan kapasitas yang sangat besar, prosesor berkecepatan tinggi, dan buffer yang sangat besar.

Hal ini merupakan asumsi logis untuk dikontrol di dalam lingkungan yang masih terbatas seperti corporate local area network (LAN). Tetapi belum tentu berlaku jika telah memasuki jaringan global seperti internet.

Model kedua dalam pemenuhan quality of service adalah *traffic engineering*. Ide dasar disini adalah bahwa trafik dapat dibeda-bedakan dan disediakan dengan tingkat layanan yang tidak harus sama. Butir-butir pembedaan tersebut berupa suatu kelas-kelas kecil (mis: prioritas sederhana). Beberapa kontrol harus ditekankan seperti berapa banyak trafik dari tiap kelas yang diijinkan memasuki jaringan, didasarkan pada sumber yang tersedia yang bisa dilakukan secara statis atau secara dinamis. Sebagai tambahan, elemen jaringan harus mengelola pemrosesan dan antrian paket dengan cara yang jelas, dan untuk paket-paket disediakan diferensiasi layanan.

Traffic engineering mempunyai dua sub kategori, yaitu:

1. Reservation-based; resource untuk trafik diidentifikasi dan dipesan secara jelas. Node-node jaringan mengklasifikasikan paket-paket yang datang dan menggunakan reservasi untuk menyediakan layanan yang berbeda.

Reservation-less; tidak ada resource yang dipesan secara pasti. Trafik didiferensiasi dalam kelas-kelas, dan node-node jaringan menyediakan perlakuan yang didasarkan pada prioritas (priority-based) pada kelas-kelas tersebut.[14]

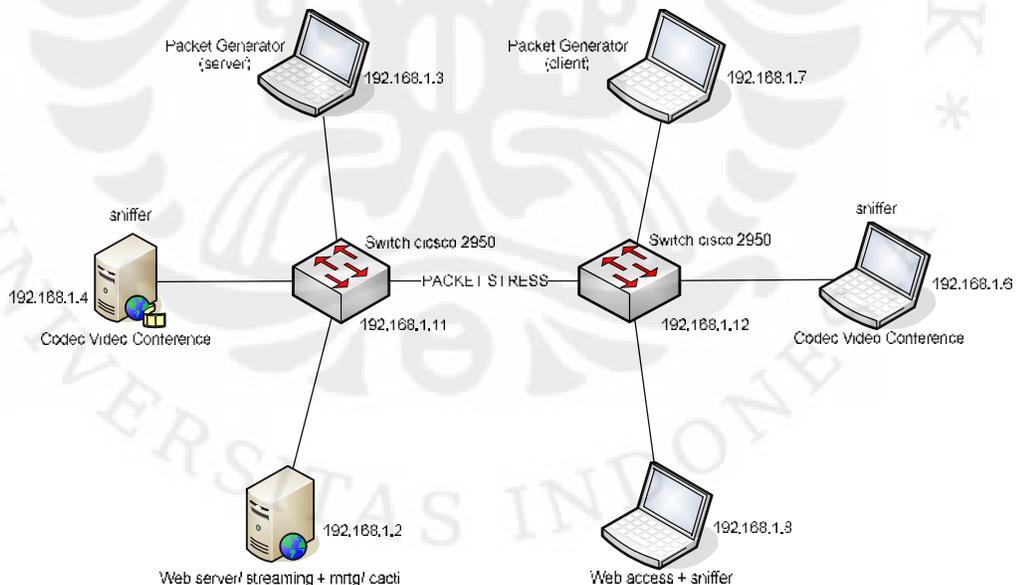
BAB 3 PERENCANAAN DAN UJICOBA

3.1 Pendahuluan

Pada bab ini akan dibahas mengenai perancangan infrastruktur yang mendukung pengukuran *Quality of Service* (QoS), instalasi, dan konfigurasi jaringan baik perangkat keras maupun perangkat lunak. Infrastruktur yang mendukung untuk skripsi ini terdiri dari dua buah Cisco Switch layer 2, dua buah komputer yang digunakan sebagai *codec video conference*, dua buah komputer untuk *traffic generator (client-server)*, 1 buah komputer sebagai *web server* dan Cacti sebagai *Bandwidth Monitoring Server*, dan satu buah komputer sebagai *sniffer* dan akses web. Untuk menghubungkan semua perangkat menggunakan kabel *Unshielded Twisted Pair* (UTP).

3.2 Topologi Jaringan

Topologi jaringan yang dilakukan untuk pengukuran *Quality of Service*,



Gambar 3.1 Topologi jaringan Video Conference

3.3 Perangkat pendukung infrastruktur

3.3.1 *Switch Layer 2*

Switch Layer 2 atau cisco catalyst merupakan perangkat yang bekerja pada layer data link. Berbeda dengan hub, switch layer 2 mampu membuat segmentasi jaringan dengan cara virtualisasi network dan tidak mem-broadcast semua paket yang dikirimkan oleh komputer ke salah satu port switch layer 2. Sehingga paket data tidak bisa diambil datanya oleh komputer lain yang tidak dalam satu segmen.

Pada skripsi ini digunakan Cisco Switch Catalyst 2950 dengan software type Enhance Image (EI) *Releases 12,1 (22)*. Switch ini digunakan sebagai bridge antar perangkat yang kemudian akan diimplementasikan *Quality of Service*. Sehingga paket data yang dianggap lebih diprioritaskan akan di lewatkan terlebih dahulu ketika bandwidth pada jaringan (trunking antar switch) telah penuh.

3.3.2 *Codec Video Conference*

Codec (*Coding and Decoding*) merupakan suatu cara untuk merubah sinyal audio atau video menjadi bit-bit digital yang kemudian akan ditransmisikan ke jaringan dalam bentuk paket IP. Pada Tugas Akhir ini digunakan codec Netmeeting. Netmeeting merupakan perangkat lunak berlisensi yang dikembangkan oleh Microsoft. Netmeeting menggunakan protokol H.323 sebagai protokol komunikasi untuk *video conference*. Pada Tugas Akhir ini digunakan netmeeting berjalan di atas windows XP dengan *input video* dan *audio* menggunakan *webcam* atau *handycam* dan *microphone optional*.

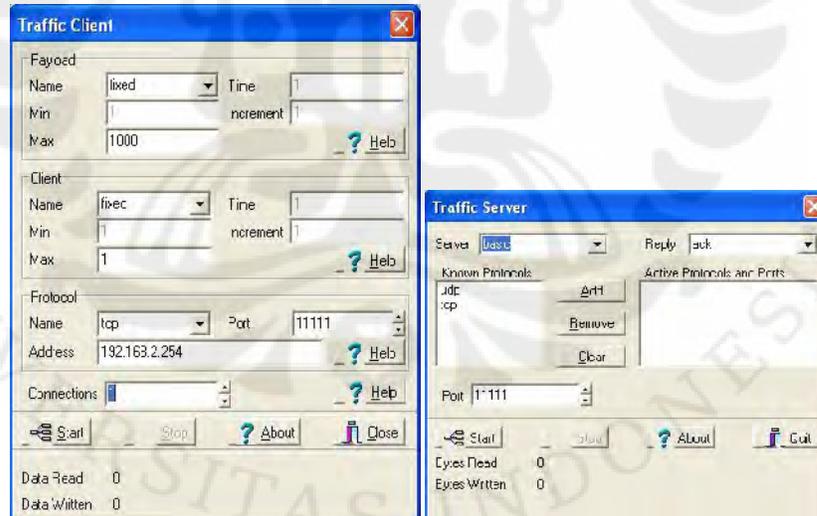
3.3.3 **Web Server**

Web Server merupakan sebuah perangkat lunak server yang berfungsi menerima permintaan *Hypertext Transfer Protocol* (HTTP atau HTTPS) dari *client* yang dikenal dengan mesin pencari (*web browser*) dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman web yang berbentuk dokumen *Hypertext Markup Language* (HTML). Halaman-halaman web mempunyai alamat *Intenet Protocol* (IP) baik *private* maupun *public* yang sering disebut dengan website sehingga client dapat mengakses halaman web dengan mengakses alamat

tersebut. Web server dapat dibangun pada berbagai platform dengan aplikasinya masing-masing. Pada skripsi ini web server berjalan di atas platform Linux Debian 5.0 (Lenny) dengan software Apache Web Server, web server ini digunakan sebagai server yang menyimpan beberapa file dengan kapasitas besar.

3.3.4 Packet Generator

Packet Generator adalah sebuah perangkat lunak yang berfungsi *generate* paket data dengan ukuran yang dapat diatur besar paket yang akan ditransmisikan dan protokol yang digunakan dalam pengiriman paket data. Packet Generator digunakan dapat digunakan untuk mengukur performance jaringan dan dapat juga digunakan untuk mengukur kehandalan sebuah aplikasi. Packet Generator yang digunakan dalam skripsi ini bersifat *client-server*, dimana packet generator client akan mengirimkan paket ke packet generator server menggunakan protokol dan port yang sesuai antara packet generator client dan packet generator server. Packet Generator digunakan dalam skripsi ini bertujuan untuk meningkatkan packet stress pada jaringan.

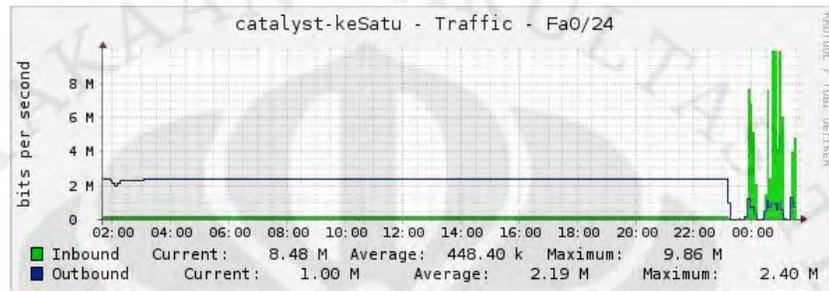


Gambar 3.2 Interface Packet Generator

3.3.5 Bandwidth Monitoring menggunakan CACTI

Cacti merupakan *front-end* dari RRDTool, cacti mengumpulkan informasi yang di butuhkan untuk pembuatan grafik dan menyimpan informasi tersebut

menjadi data dalam *database* Mysql. *Front-end* tersebut dibuat sepenuhnya menggunakan bahasa pemrograman PHP. Selain kemampuan untuk menginterpretasikan grafik, *Data Sources* dan *Round Robin* arsip dalam *database* dapat menhandel pengumpulan data. Data-data ini dapat di visualisasikan sehingga dapat dibaca oleh manusia untuk *monitoring traffic*, utilisasi server dan lain-lain.



Gambar 3.3 monitoring port 24 cisco catalyst

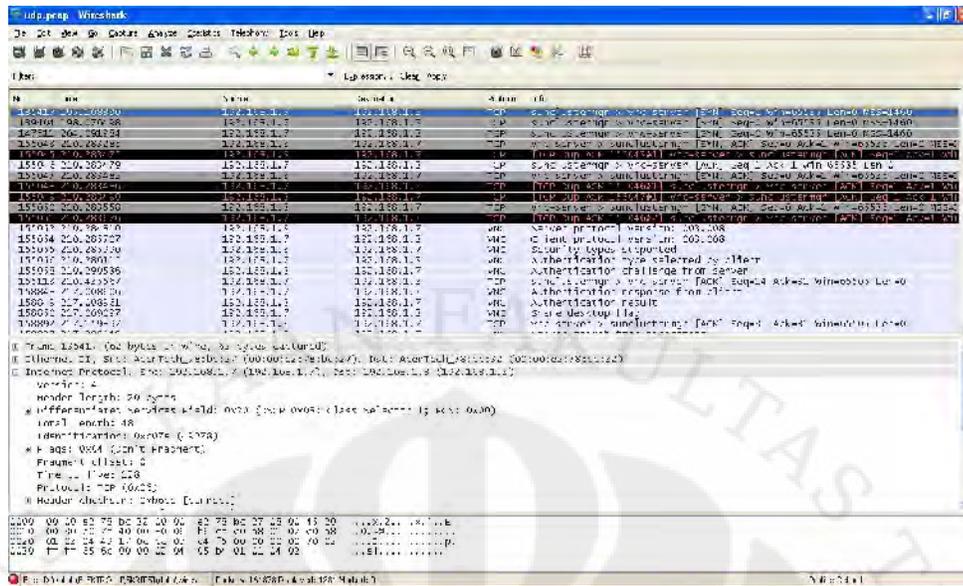
Keterangan Gambar:

Inbound: Traffic port input

Outbound: Traffic port Output

3.3.6 Packet Sniffer menggunakan Wireshark

Packet Sniffer merupakan sebuah cara untuk menganalisa (packet analyzer) kondisi jaringan komputer. Pada skripsi ini digunakan Wireshark sebagai tools Packet Sniffer. Wireshark mampu menangkap paket-paket data/informasi yang berseliweran dalam jaringan yang akan dianalisa. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tool* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya.



Gambar 3.4 Interface Wireshark

3.4 Instalasi infrastruktur

Pada bagian ini akan dijelaskan rancangan dari proses yang akan dilakukan pada instalasi perangkat keras dan perangkat lunak pendukung jaringan yang akan digunakan pada implementasi *Video Conference*.

3.4.1 Instalasi *Switch Layer 2 Cisco 2950*

Switch cisco 2950 merupakan *switch* yang dapat diatur (*managable*) dimana setiap port nya bisa dikonfigurasi sesuai dengan kebutuhan jaringan. Pada perancangan skripsi ini, *Switch Layer 2* tidak digunakan untuk segmentasi jaringan karena kebutuhan jaringan relatif sederhana. *Switch Layer 2* dapat digunakan untuk memprioritaskan aliran paket yang melalui *switch* sehingga paket data yang dianggap lebih penting dapat diprioritaskan dalam jaringan. Berikut ini adalah kemampuan cisco *switch* layer 2 tipe 2950 dengan IOS *Enhance Image (EI) V 12.1*

1. *Classification*

Mengklasifikasikan segmen IP address berdasarkan *access-list*

2. *Marking*

Membuat Penandaan (*tagging*) pada *access-list* yang telah dibuat

3. Policing

Melakukan pengaturan prioritas untuk segmen IP address yang telah ditandai.

4. Mapping

Pemetaan nilai-nilai *Quality of Service*

5. Queuing and scheduling

Membuat penjadwalan atas semua *Class of Service* pada port keluaran.

Untuk konfigurasi *Switch Cisco Catalyst* dapat dilihat pada lampiran 1.

3.4.2 Instalasi Codec Video Conference

Secara default Netmeeting sudah include dengan Windows system tinggal kita lakukan install, sedang pada Windows XP software NetMeeting-nya menggunakan versi 3.01. Proses instalasi Windows NetMeeting sebagai berikut:

- Klik Start → Run → ketik conf → Enter



Gambar 3.5 Memulai install NetMeeting

- Klik Next (menjelaskan fungsi dari NetMeeting)



Gambar 3.6 Menjelaskan fungsi dari NetMeeting

- Kemudian memasukkan data client sesuai dengan kolom isian untuk kolom nama akan digunakan sebagai nickname, selanjutnya Klik Next.

- ♦ Pilih spesifikasi koneksi yang dipakai yaitu Local Area Network, selanjutnya Klik Next.
- ♦ Selanjutnya klik Next, untuk melakukan pengecekan fungsi dari speaker, microphone dan camera.
- ♦ Proses Install NetMeeting selesai , selanjutnya Klik Finish dan aplikasi NetMeeting sudah bisa dijalankan:



Gambar 3.7 Interface NetMeeting

3.4.3 Instalasi Cacti

Instalasi cacti secara lengkap bisa dilihat di lampiran 1

3.4.4 Instalasi Packet Generator

Packet Generator pada skripsi berjalan di atas sistem operasi windows. *Packet Generator Server* dan *Packet Generator Client* tergabung dalam satu *Installer*. Untuk instalasinya cukup sederhana. Klik dua kali pada software installer kemudian ikuti petunjuk selanjutnya. Dan untuk pertama kali menjalankan akan diberikan pilihan apakah akan menjalankan *Packet Generator Server* atau *Packet Generator Client*.

3.4.5 Instalasi Web Server

Web Server pada skripsi berjalan pada sistem operasi Linux distro Debian 5.0 (Lenny). Software yang digunakan sebagai web server pada skripsi ini adalah Apache 2.0. cara instalasinya cukup mudah. Setelah network dan link repositori Linux telah disetting, maka cukup menggunakan command “apt-get install apache2”, maka apache 2 akan terinstall secara otomatis.

3.4.6 Instalasi Wireshark

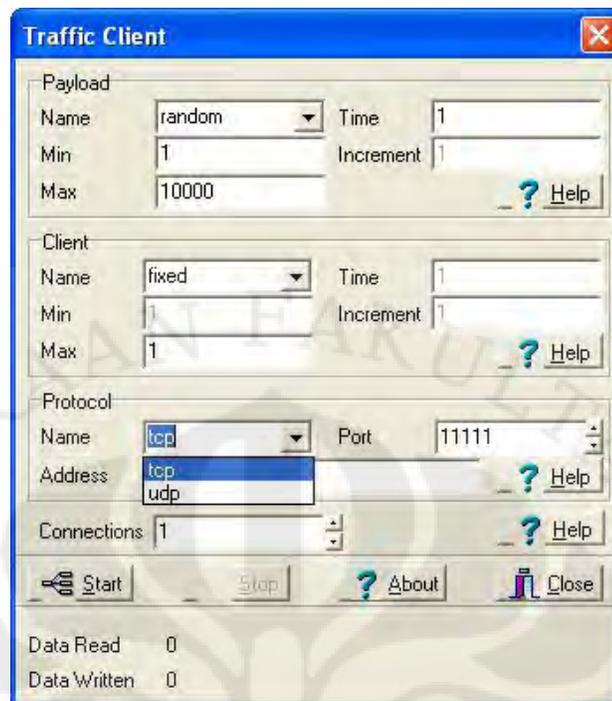
Instalasi Wireshark pada windows relatif sederhana. Klik dua kali Wireshark Installer, kemudian ikuti langkah berikutnya sampai selesai.

3.5 Pengukuran *Quality of Service*

Pada Tugas Akhir ini akan dilakukan beberapa tahap ujicoba dengan tujuan untuk mendapatkan beberapa perbandingan data hasil pengukuran. Ada tiga aplikasi yang dijalankan yaitu video conference, website, dan packet generator. Adapun pengukuran dilakukan sebanyak enam tahap.

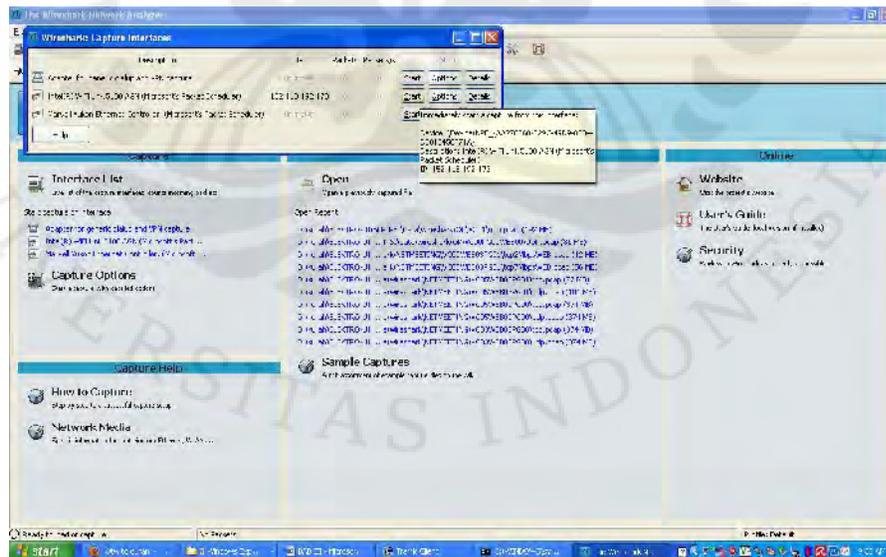
3.5.1 Petunjuk Ujicoba Ketika Belum Implementasi QoS pada Switch layer 2

Ujicoba yang pertama adalah menjalankan semua aplikasi yaitu *video conference*, *packet generator*, dan *download* ke webserver. Pada aplikasi packet generator disetting transport protokolnya menjadi UDP dan TCP.



Gambar 3.8 Setting Packet Generator Client

Kemudian menjalankan wireshark untuk meng-capture paket yang melewati port 24 switch catalyst yang telah di-mirror ke port ketiga



Gambar 3.9 Langkah menjalankan Wireshark

Sebelum menjalankan Aplikasi Video Conference maka sniff paket UDP maka dijalankan terlebih dahulu Wireshark pada dua sisi yaitu *endpoint* pertama dan

end point kedua sehingga *request packet* dan *acknowledgement* dari protokol H.323 dapat dibaca. Setelah wireshark dijalankan, panggil endpoint kedua (oleh endpoint pertama).



Gambar 3.10 memanggil IP endpoint

3.5.2 Petunjuk Ujicoba Ketika Video Conference disetting kelas Satu

Untuk uji coba yang kedua dan selanjutnya pada prinsipnya sama yaitu menghidupkan wireshark sebagai sniffer terlebih dahulu sebelum semua aplikasi dan paket generator dibuat UDP dan TCP dijalankan. Akan tetapi di perangkat switch catalyst di konfigurasi Quality of service yang memprioritaskan paket video conference sehingga diharapkan kualitas video conference akan lebih bagus. Di bawah ini adalah konfigurasi switch catalyst 2950.

```
CSS-2950T-kedua(config)#access-list 1 permit host 192.168.1.4
```

```
CSS-2950T-kedua(config)#class-map ipclass1
```

```
CSS-2950T-kedua(config-cmap)#match access-group 1
```

```
CSS-2950T-kedua(config-cmap)#exit
```

```
CSS-2950T-kedua(config)#policy-map flow1t
```

```
CSS-2950T-kedua(config-pmap)#class ipclass1
```

```
CSS-2950T-kedu(config-pmap-c)#set ip dscp 8
```

```
CSS-2950T-kedu(config-pmap-c)#exit
```

```
CSS-2950T-kedua(config-pmap)#exit
```

```
CSS-2950T-kedua(config)#int fa0/3
```

```
CSS-2950T-kedua(config-if)#service-policy input flow1t
```

```
CSS-2950T-kedua(config-if)#end
```

3.5.2 Petunjuk Ujicoba Ketika Video Conference disetting kelas Tiga

Untuk ujicoba yang ketiga yaitu dengan mengkonfigurasi switch catalyst agar paket video conference menjadi kelas 3. Kemudian menjalankan semua aplikasi dan capture paket menggunakan wireshark. Untuk konfigurasi switch bisa dilihat di lampiran 1

3.5.2 Petunjuk Ujicoba Ketika Video Conference disetting kelas Lima

Untuk ujicoba yang keempat yaitu dengan mengkonfigurasi switch catalyst agar paket video conference menjadi kelas lima. Kemudian menjalankan semua aplikasi dan capture paket menggunakan wireshark.

3.5.5 Petunjuk Ujicoba Ketika Packet Generator disetting kelas lima, Website kelas tiga, dan Video Conference kelas satu.

Uji coba yang kelima adalah membuat klasifikasi semua paket yang lewat kemudian di-capture menggunakan wireshark. Konfigurasi switch bisa dilihat di lampiran 1

3.5.6 Petunjuk Ujicoba Ketika Packet Generator disetting kelas lima, Website kelas tiga, dan Video Conference tidak diset kelas

Untuk uji coba yang terakhir adalah dengan mengkonfigurasi switch dimana Packet Generator menjadi kelas ketiga, website menjadi kelas pertama, sedangkan video conference (vicon) tidak disetting QoSnya. Langkah percobaannya adalah dengan menjalankan packet generator dan website terlebih dahulu, kemudian menjalankan wireshark pada komputer yang digunakan untuk video conference (vicon), baru kemudian menjalankan video conference sehingga paket *request* (SYN) dan *acknowledgement* (ACK) aplikasi video conference dapat terlihat pada wireshark. Untuk konfigurasi switch dapat terlihat di lampiran 1.

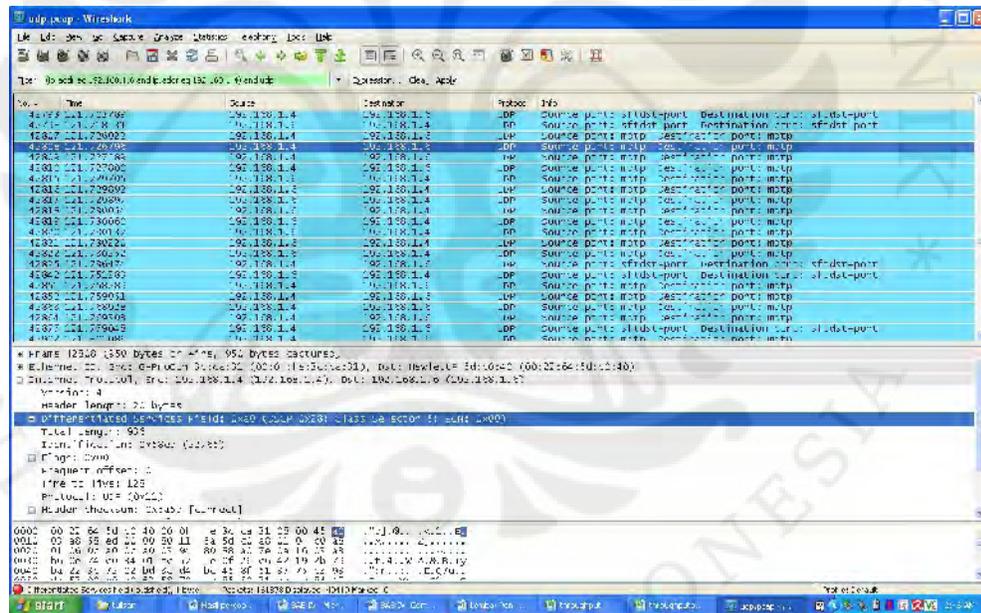
BAB 4

HASIL PENGUKURAN DAN ANALISIS DATA

Pada BAB ini akan dibahas analisis tentang performansi jaringan IP pada *switch layer 2* untuk aplikasi *Video Conference* dengan protocol UDP, analisis yang dilakukan meliputi pengamatan paket, *delay end to end*, *bandwidth*, *throughput* jaringan serta kualitas dari gambar dan suara ketika dilakukan klasifikasi *Quality of Service (QoS)* pada *switch cisco 2950*.

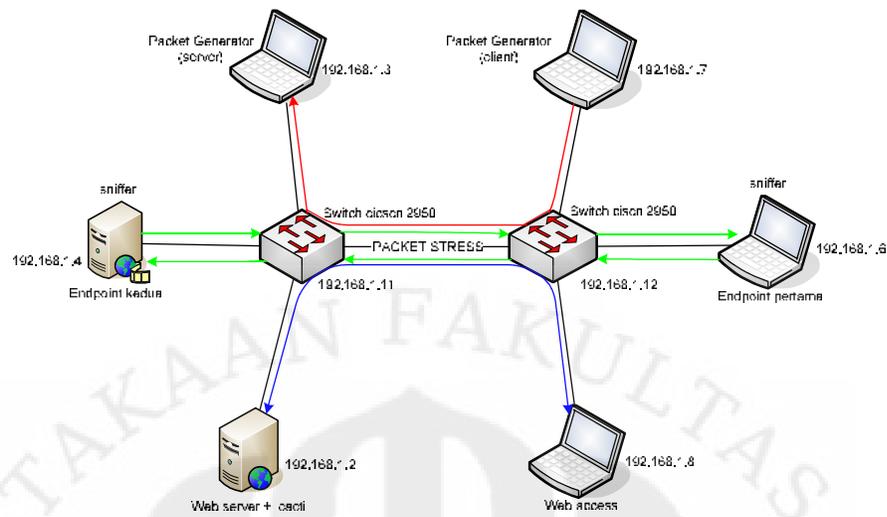
4.1 Pengamatan Paket

Untuk melihat bahwa prioritas paket sudah terjadi, maka dapat dilihat pada field layer tiga (Internet Layer) yaitu pada *field Differentiated Services* seperti terlihat pada *gambar 4.1*



Gambar 4.1 Field Differentiated Services

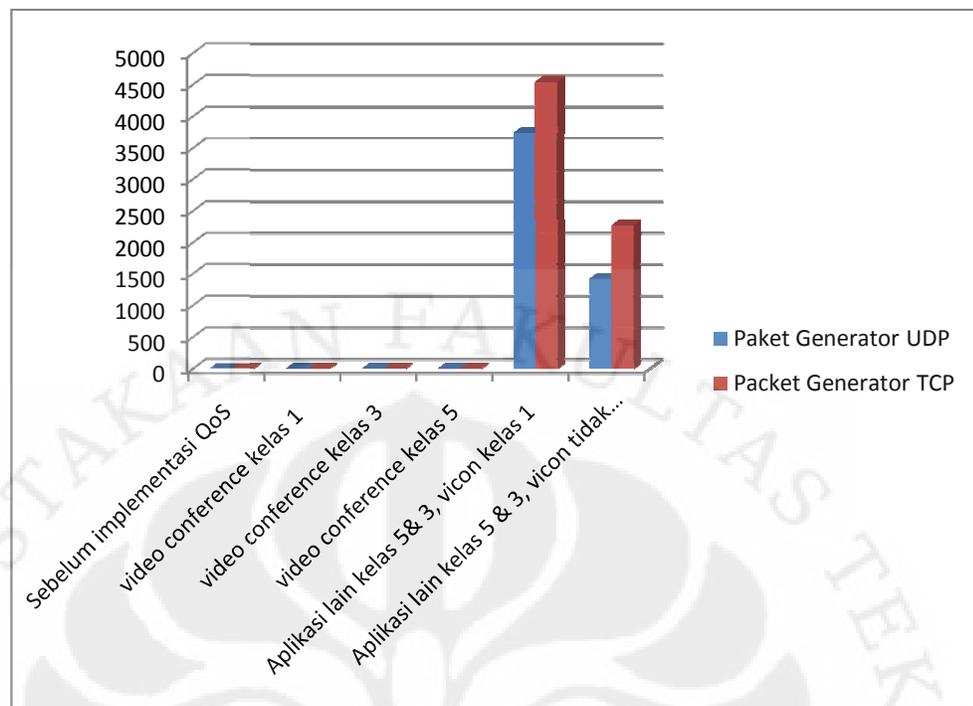
Gambar diatas menunjukkan bahwa paket *video conference* (vicon) dengan Source IP 192.168.1.4 dan destination IP 192.168.1.6 dengan protocol transport UDP diklasifikasikan pada kelas 5 yaitu dengan nilai *Differentated Services Code Point (DSCP)* 28. Kelas 5 pada penelitian ini adalah kelas yang paling tinggi dimana egress port queue pada switch diberikan prioritas tertinggi. Lebih jelas konfigurasi *switch* bisa melihat di Lampiran 1.



Gambar 4.2 Traffic flow Uji coba

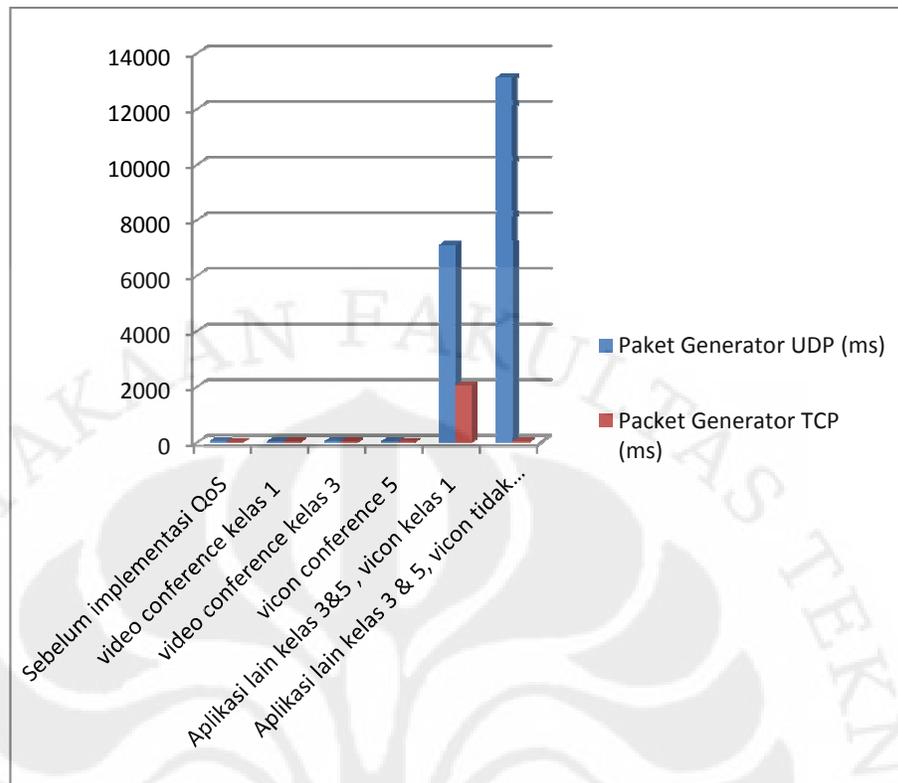
Gambar 4.2 di atas menunjukkan *traffic flow* pada uji coba. Pengamatan paket pada penelitian ini dilakukan dengan cara mengamati jumlah paket yang dikirimkan maupun yang diterima oleh masing-masing *endpoint* yang melalui protokol TCP/IP dan yang sangat penting dalam pengamatan paket adalah adanya paket loss saat melakukan komunikasi aplikasi *Video Conference* (Vicon). Karena saat terjadi paket loss suara dan gambar yang terjadi pada sisi penerima menjadi terputus – putus,

Loss packet (kehilangan paket) terjadi ketika *peak load* dan *congestion* (kemacetan transmisi paket akibat padatnya *traffic* yang harus dilayani) dalam batas waktu tertentu, maka *frame* (gabungan data *payload* dan *header* yang di transmisikan) suara akan dibuang sebagaimana perlakuan terhadap *frame* data lainnya pada jaringan berbasis IP.



Gambar 4.3 Grafik hasil perhitungan packet loss

Gambar 4.3 menunjukkan bahwa ketika switch 2950 belum dikonfigurasi QoS, maka tidak terjadi paket loss meskipun jalur interkoneksi antar switch sudah penuh, hal ini terjadi karena meskipun pada switch tidak dikonfigurasi, aplikasi video conference secara default mendefinisikan diri menjadi kelas 3 atau 5. Ketika input paket video conference di setting menjadi kelas 1 sampai kelas 5 juga belum terjadi packet loss, namun pada saat port service aplikasi yang lain didefinisikan kelas, maka aplikasi video conference akan turun kualitasnya yaitu dengan paket loss sebesar 4000 paket dari sekitar 18000 paket yang lewat, atau bisa dikatakan besar *fraction loss*-nya adalah 22,22 %, dan ketika video conference tidak didefinisikan kelasnya maka *fraction loss* atau packet loss akan menurun karena aplikasi video conference menempatkan dirinya pada kelas 3 atau DSCP 18.

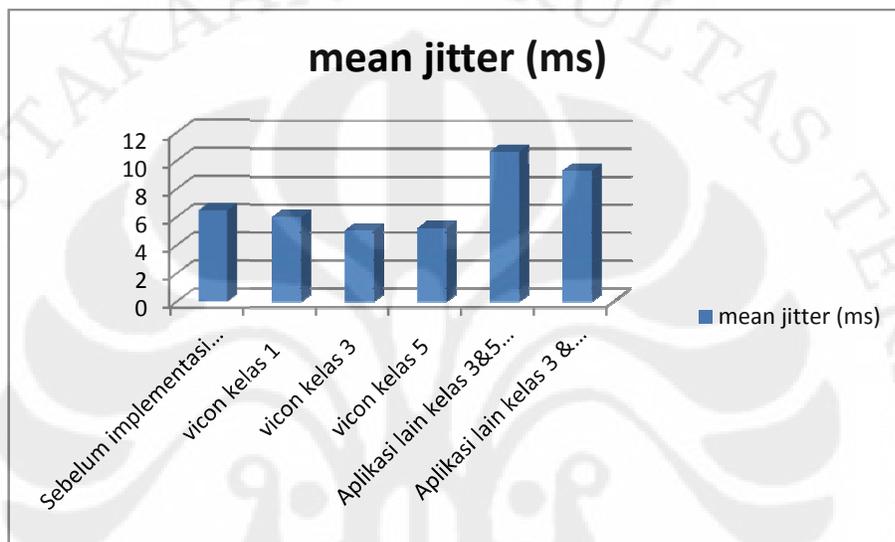


Gambar 4.5 Grafik Hasil Perhitungan Delay

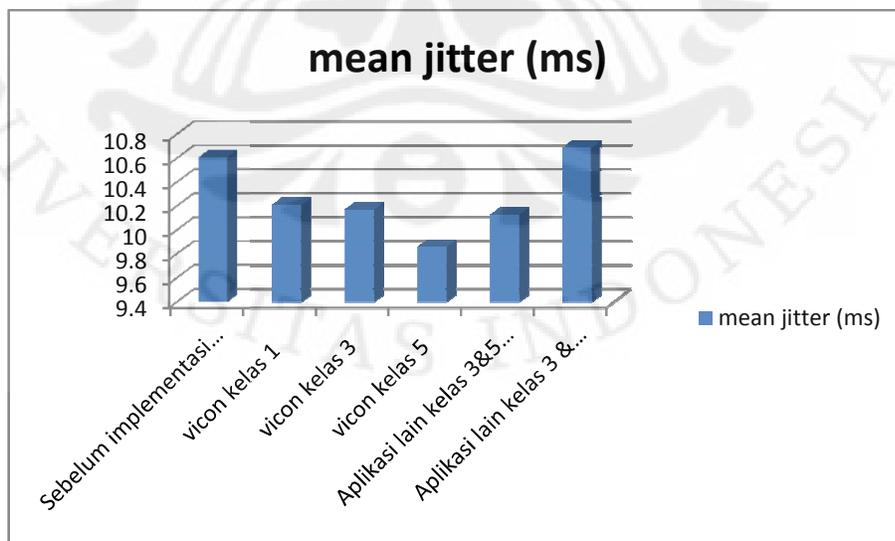
Dari gambar 4.5 di atas dapat dianalisa bahwa ketika paket video conference belum didefinisikan QoS secara pribadi telah mendefinisikan sendiri menjadi kelas 3 atau kelas 5 dan juga pada kondisi ini tidak terjadi indikasi packet loss karena path interkoneksi sangat pendek dan atau karena hanya ada dua hop, sehingga apabila terjadi retransmisi packet yang hilang tidak membutuhkan waktu yang lama. Begitu juga pada saat paket video conference didefinisikan pada kelas 1, kelas 3, dan kelas 5 tidak terjadi delay sama sekali. Namun pada saat aplikasi lain didefinisikan kelas yang lebih tinggi yaitu kelas 3 dan kelas 5, maka terjadi delay yang sangat signifikan, namun perhitungan ini adalah perhitungan rata-rata yang artinya bahwa delay terjadi tidak terus-menerus, delay tinggi ini terjadi hanya beberapa saat (detik) kemudian gambar yang sebelumnya freeze karena pengaruh delay akan menjadi normal, dan pada suatu saat akan kembali terjadi delay kembali. Untuk melihat selengkapnya hasil perhitungan delay bisa dilihat pada Lampiran 2.

4.3 Pengukuran Jitter

Paket video conference sebelum dikirimkan melalui layer transport oleh UDP diberikan header *Real Time Protocol (RTP)* yang terdiri dari 16 byte dimana 4 byte mendefinisikan *Timestamp* yang dapat digunakan untuk sinkronisasi paket dan menghitung delay. Tabel hasil pengukuran jitter selengkapnya dapat dilihat pada lampiran 2.



Gambar 4.6 Grafik Mean Jitter pada endpoint pertama



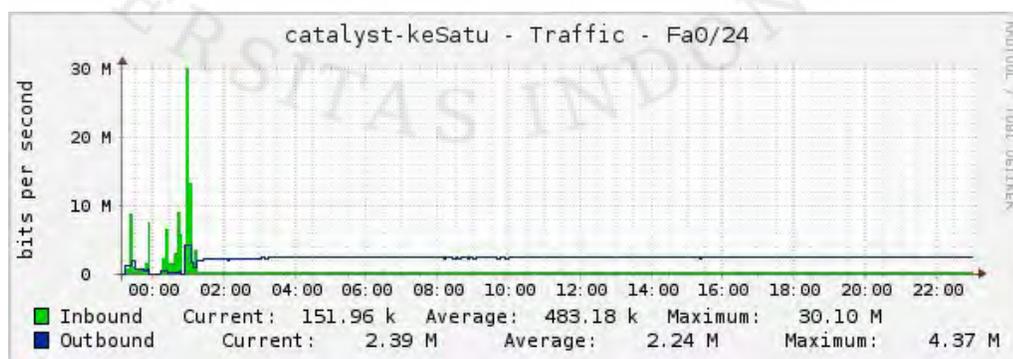
Gambar 4.7 Grafik Mean Jitter pada endpoint kedua

Grafik gambar 4.7 dan gambar 4.8 merupakan hasil perhitungan jitter yang di *capture* pada *endpoint codec video conference*. Dari grafik di atas dapat dianalisa bahwa ketika *switch* belum dikonfigurasi QoSnya, maka nilai jitter 6,49 ms pada endpoint pertama dan 10,61 ms pada endpoint yang kedua. Ketika switch dikonfigurasi QoS untuk paket video conference, maka akan menurunkan jitter yang cukup besar, yaitu seperti pada endpoint yang kedua, pada saat belum dikonfigurasi dan pada saat aplikasi lain didefinisikan kelas 3 dan kelas 5 maka terjadi jitter sebesar 10,68 ms sedangkan pada saat paket video conference didefinisikan kelas 5, maka nilai jitter menjadi 9,86 ms. Perubahan jitter dinilai besar karena jaringan video conference bersifat local.

4.4 Pengukuran Bandwidth

Bandwidth adalah kecepatan maksimum yang dapat digunakan untuk melakukan transmisi data antar komputer pada jaringan IP atau internet. Dalam perancangan *Video Conference*, bandwidth merupakan bagian yang harus diperhitungkan agar dapat memenuhi kebutuhan pengguna, yang digunakan sebagai parameter untuk menghitung kebutuhan infrastruktur jaringan yang akan dipakai. Perhitungan ini juga sangat diperlukan dalam efisiensi jaringan dan biaya serta sebagai acuan pemenuhan kebutuhan untuk pengembangan di masa mendatang. Packet loss (kehilangan paket data pada proses transmisi) merupakan masalah yang berhubungan dengan kebutuhan bandwidth.

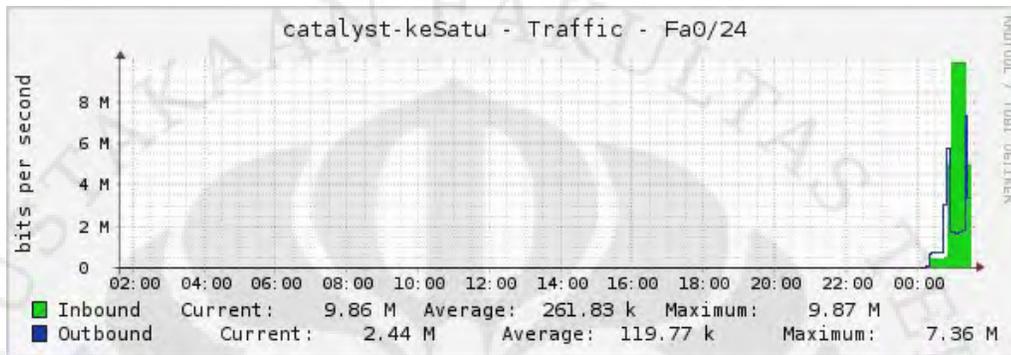
Secara *default* switch cisco catalyst 2950 mempunyai kecepatan akses sampai dengan 100 Mbps (*fast ethernet*).



Gambar 4.8 Traffic tiga aplikasi pada port fast ethernet switch catalyst

Apabila semua aplikasi dijalankan, maka bandwidth yang digunakan adalah lebih dari 30 Mbps. Sehingga pada kondisi ini kualitas video conference menjadi sangat jernih dan kecepatan download akan menjadi maksimal.

Port interface catalyst 2950 dapat dibuat menjadi 10 Mbps sehingga akan terjadi buffering pada switch cisco 2950 ketika paket yang datang lebih dari 10 Mbps

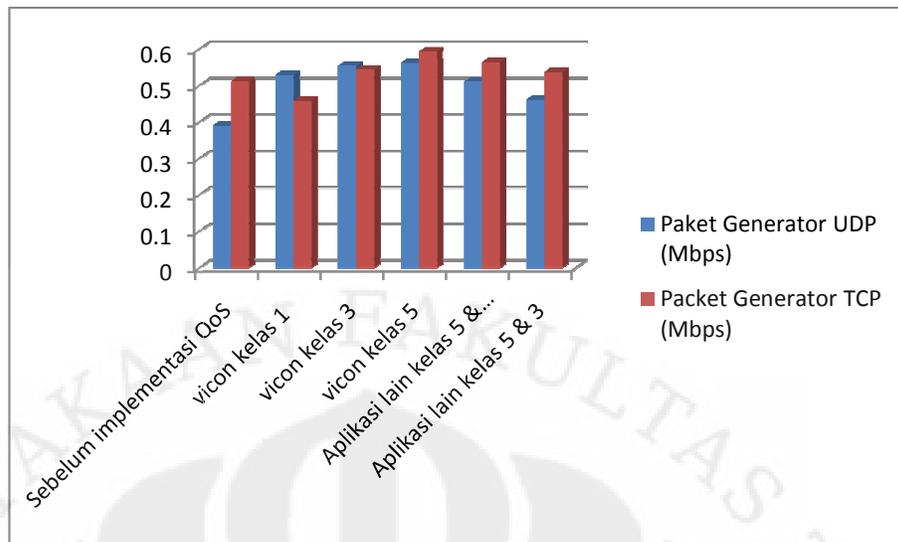


Gambar 4.9 Traffic tiga aplikasi pada port 10 Mbps switch catalyst

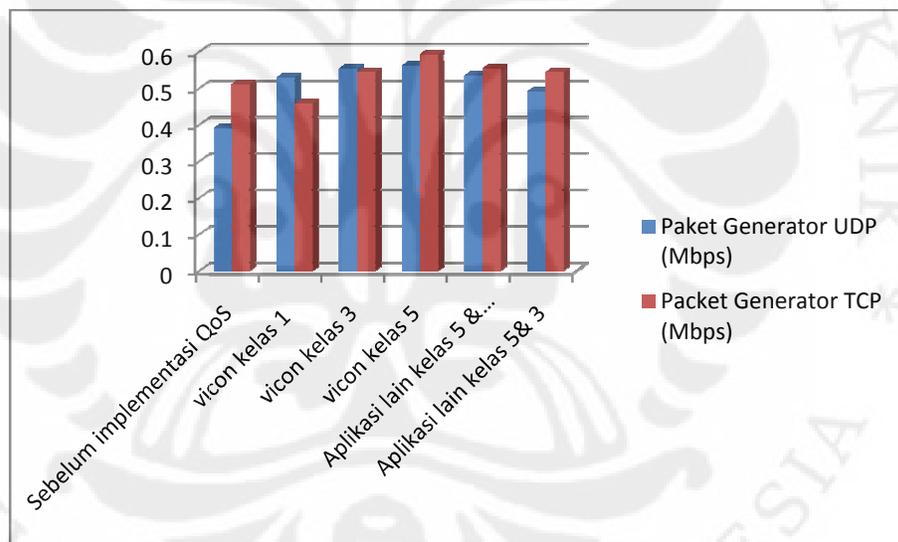
Pada kondisi ini prioritas paket yang melewati switch catalyst sangat dibutuhkan sehingga aplikasi yang rentan terhadap delay, jitter dan packet loss tetap dalam kondisi baik.

4.5 Pengukuran Throughput

Throughput adalah jumlah bit yang ditransmisikan perdetik melalui sebuah sistem atau media komunikasi. Throughput diukur setelah transmisi data (host/client) karena suatu sistem akan menambah delay yang disebabkan *processor limitations*, kongesti jaringan, *buffering inefficients*, error transmisi, *traffic loads* atau mungkin desain hardware yang tidak mencukupi. Aspek utama throughput yaitu berkisar pada ketersediaan bandwidth yang cukup untuk menjalankan aplikasi. Hal ini menentukan besarnya trafik yang dapat diperoleh suatu aplikasi saat melewati jaringan. Aspek penting lainnya adalah error (pada umumnya berhubungan dengan link error rate) dan losses (pada umumnya berhubungan dengan kapasitas buffer).



Gambar 4.10 Grafik Throughput pada endpoint pertama



Gambar 4.11 Grafik Throughput pada endpoint kedua

Dari gambar terlihat bahwa throughput video conference meningkat ketika switch 2950 dikonfigurasi yang memberikan kelas 5 pada aplikasi video conference, dan throughput akan lebih besar apabila pembebanan oleh paket TCP.

BAB 5

KESIMPULAN

Berdasarkan hasil pembahasan pada bab-bab sebelumnya, berikut hasil beberapa kesimpulan yang dapat ditarik dari tugas akhir ini:

1. Setelah bandwidth interkoneksi switch catalyst 2950 diturunkan dari 100 Mbps menjadi 10 Mbps, terjadi antrian paket sehingga kualitas video conference menurun.
2. Pada saat paket video conference tidak didefinisikan dan paket aplikasi lain didefinisikan kelas 3 dan 5, terjadi jitter maksimal sebesar 7400,86 ms pada video protocol H.263 dan jitter sebesar 2963,02 ms pada audio protocol G.723 yang menyebabkan gambar dan suara patah-patah.
3. Pada saat switch cisco catalyst 2950 tidak dikonfigurasi QoS, paket video conference secara default memilih class selector 3 atau *Differentiated Services Code Point (DSCP) 28*.
4. Maksimum packet loss terjadi pada saat paket video conference di masukan pada kelas 1 dan aplikasi lain pada kelas 3 dan kelas 5, yaitu sebesar 4555 paket dari 17831 total paket yang lewat.
5. Throughput aplikasi video conference relative besar yaitu 0,594 Mbps pada saat paket didefinisikan pada kelas 5. Dan throughput maksimum ini terjadi pada saat pembebanan traffic oleh packet generator menggunakan protocol TCP.
6. Pada saat Video Conference diset pada kelas 1 dan aplikasi website pada kelas 3 dan Packet Generator pada kelas 5 didapatkan delay sebesar 7086 ms.
7. Berdasarkan hasil penelitian, maka kondisi terbaik adalah ketika trafik video conference tidak perlu di definisikan kelasnya karena secara default telah mendefinisikan diri pada kelas tiga dan paket website dan packet generator didefinisikan pada kelas dibawahnya yaitu kelas satu, hal ini sama seperti yang telah direkomendasikan oleh Cisco Sytem.

DAFTAR REFERENSI

- [1] Supriyadi, Andi., & Gartina, Dhani. “Memilih Topologi Jaringan dan Hardware dalam Desain Sebuah Jaringan Komputer”. Informatika Pertanian volume 16 No.2, 2007.
- [2] “Switching Path Overview”. 2009, August.
<http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdovips.html>
- [3] “Unshielded Twisted Pair”. 2009, August.
<http://www.firewall.cx/cabling_utp.php>
- [4] “Konsep Dasar TCP”. Juli 2009.
<www.oke.or.id/tutorial/Konsep%20Dasar%20TCP.doc>
- [5] “Internet Communications Engineering – A Tutorial”. 2009, September.
<<http://www.erg.abdn.ac.uk/users/gorry/course>>
- [6] “RTP, Real-time Control Protocol”. RFC Sourcebook. 2009, June.
<<http://www.networksorcery.com/enp/protocol/rtp.htm>>
- [7] “Sekilas Tentang Cacti”. Juli 2009.
<<http://blog.afri.web.id/index.php/2009/06/10/sekilas-tentang-cacti/>>
- [8] “Kebutuhan Infrastruktur Untuk Video Conference”. Mei 2009.
<www.onno.vlsm.org/v11/onno-ind-3/network/kebutuhan-infrastruktur-untuk-video-conference-3-2003.rtf>
- [9] “G.7xx: Audio (Voice) Compression Protocols (CODEC) (G.711, G.721, G.722, G.726, G.727, G.728, G.729)”. 2009, October.
<<http://www.javvin.com/protocolG7xx.html>>
- [10] “IT Corner. Kebutuhan Bandwidth Video”. Juli 2009.
<<http://victorgm.blogspot.com/2008/05/kebutuhan-bandwidth-video.html>>
- [11] “H.323 Multimedia Conferencing Standard”. 2009, August.
<<http://www.linktionary.com/h/h323.html>>
- [12] Garcia, Albert. “QOS For IP Video Conference”. System Engineer, Cisco System. 11/14/2001.

[13] “Configuring QoS”. 2009, November.

http://www.cisco.com.ru/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/swqos.html

[14] Syafa’ah, Lailis.” *Study Penerapan QoS (QUALITY OF SERVICE) Melalui Jaringan Multiprotocol Labels Switching (MPLS) Pada Internet Protocol (IP)*”. Jurusan Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Malang.



Lampiran 1. *Setting* dan Konfigurasi Perangkat

Konfigurasi Switch Cisco Catalyst 2950

```
CSS-2950-kesatu>enable
```

Log in sebagai privilege user

```
CSS-2950#conf t
```

Masuk menu konfigurasi

```
CSS-2950-kesatu(config)#snmp-server community public rw
```

Konfigurasi snmp-server agar bisa di monitor oleh Cacti

```
CSS-2950-kesatu(config)#int fa0/3
```

```
CSS-2950-kesatu(config-if)#port monitor fa0/24
```

```
CSS-2950-kesatu(config-if)#end
```

```
CSS-2950-kesatu#show monitor
```

```
Session 1
```

```
-----
```

```
Type          : Local Session
```

```
Source Ports  :
```

Both : Fa0/24

Destination Ports : Fa0/3

Encapsulation : Native

Ingress: Disabled

Konfigurasi di atas menunjukkan bahwa port 24 di-mirror ke port 3

CSS-2950T-kesatu(config)#access-list 1 permit host 192.168.1.4

Membuat akses list 1 untuk IP address 192.168.1.4 (codec video conference)

CSS-2950T-kesatu(config)#class-map ipclass1

CSS-2950T-kesatu(config-cmap)#match access-group 1

Membuat nama kelas “ipclass1” kemudian men-tag access list 1 ke ipclass1

CSS-2950T-kesatu(config-cmap)#exit

CSS-2950T-kesatu(config)#policy-map flow1

CSS-2950T-kesatu(config-pmap)#class ipclass1

CSS-2950T-kesatu(config-pmap-c)#set ip dscp 8

Membuat *policy class of service*

CSS-2950T-kesatu(config-pmap-c)#exit

```
CSS-2950T-kesatu(config-pmap)#exit
```

```
CSS-2950T-kesatu(config)#int fa0/3
```

```
CSS-2950T-kesatu(config-if)#service-policy input flow1t
```

Menentukan port input berdasarkan *policy* yang telah dibuat

```
CSS-2950T-kesatu(config-if)#end
```

```
CSS-2950T-kesatu#
```

```
CSS-2950T-kesatu#sh mls qos maps
```

```
Dscp-cos map:
```

```
dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56
```

```
-----  
cos: 0 1 1 2 2 3 3 4 4 5 5 6 7
```

```
Cos-dscp map:
```

```
cos: 0 1 2 3 4 5 6 7
```

```
-----
```

dscp: 0 8 16 26 32 46 56 48

Mapping nilai Class of Service (CoS) dengan Differentiated Services Code Point (DSCP)

CSS-2950T-kesatu(config)#wrr-queue 4 5

CSS-2950T-kesatu(config)#wrr-queue 3 4 6 7

CSS-2950T-kesatu(config)#wrr-queue 2 2 3

CSS-2950T-kesatu(config)#wrr-queue 1 0 1

Mapping Queue pada port keluaran.



Berikut ini adalah langkah-langkah instalasi cacti pada sistem operasi Debian 5.0

1. Install cacti dengan menggunakan apt-get (auto)

```
Debian:~#apt-get install cacti
```

2. Instalasi database Mysql-server

```
Debian:~#apt-get install mysql-server
```

MySQL awalnya hanya mengizinkan koneksi dari localhost (127.0.0.1) saja, untuk itu pembatasan ini harus dihapus jika ingin membuat MySQL dapat diakses oleh siapapun melalui internet. Buka berkas /etc/mysql/my.cnf

```
Debian:~#vim /etc/mysql/my.cnf
```

Cari baris ini bind-address = 127.0.0.1 dan berikan komentar (#)

...

```
#bind-address = 127.0.0.1
```

...

Default-nya MySQL tidak memasang password root. Hal ini dapat menimbulkan masalah keamanan, untuk itu dianjurkan untuk membuat password untuk root

```
Debian:~#mysqladmin -u root password your-new-password
```

```
Debian:~#mysqladmin -h root@nama-mesin-lokal -u root -p password  
your-new-password
```

```
Debian:~#sudo /etc/init.d/mysql restart
```

Sampai disini install mysql sudah selesai.

Menginstall server http Apache

```
Debian:~#apt-get install apache2
```

Setelah proses instalasi selesai, untuk mencobanya ketikan perintah ini di browser : <http://localhost>

Instalasi PHP5 untuk Server HTTP Apache

```
Debian:~#sudo apt-get install php5
```

```
Debian:~#sudo apt-get install libapache2-mod-php5
```

```
Debian:~#sudo /etc/init.d/apache2 restart
```

Untuk menguji jika php5 telah terinstal dengan baik

```
Debian:~#vim /var/www/testphp.php
```

Buat berkas baru dan masukkan baris berikut

```
<?php phpinfo(); ?>
```

Simpan berkas yang telah disunting

Untuk mengujinya, buka browser dan ketikan perintah ini

```
http://localhost/testphp.php
```

apabila belum jalan coba ketikan seperti ini

```
http://ipAddressServer/testphp.php
```

Instalasi MYSQL untuk Server HTTP Apache

```
Debian:~#apt-get install libapache2-mod-auth-mysql
```

```
Debian:~#apt-get install php5-mysql
```

Untuk membuat PHP bekerja dengan MySQL, buka berkas

```
Debian:~#vim /etc/php5/apache2/php.ini
```

Hapus komentar di baris “;extension=mysql.so” sehingga akan terlihat seperti ini

...

```
extension=mysql.so
```

...

Simpan berkas dan keluar

```
Debian:~/etc/init.d/apache2 restart
```

Untuk mempermudah penggunaan php disarankan untuk menggunakan program yang namanya “phpmyadmin” cara install di debian sbb:

```
Debian:~#apt-get install phpmyadmin
```

Setelah instalasi selesai, coba jalankan browser dan ketikkan

```
http://localhost/phpmyadmin
```

Nama pengguna : root

Kata Sandi : password_anda

Sejauh ini install paket-paket yang di butuhkan oleh si cacti sudah selesai, sekarang tibalah saatnya untuk mengkonfigurasi si cacti.

3. Konfigurasi Cacti

Membuat user untuk Cacti

```
Debian:~#adduser cacti
```

Membuat MySql database untuk cacti

```
Debian:~#mysqladmin -user=root create cacti
```

Mengimport database default si cacti

```
Debian:~#mysql cacti < cacti.sql
```

Atau bisa juga menggunakan cara barikut ini

```
Debian:~#zcat /usr/share/doc/cacti.log.gz | mysql -u root -password=cacti  
cacti
```

Membuat MySQL username dan password buat si Cacti

```
Debian:~#mysql -user=root mysql
```

```
Debian:~#mysql> GRANT ALL ON cacti.* TO cactiuser@localhost  
IDENTIFIED BY 'somepassword';
```

```
Debian:~#mysql> flush privileges;
```

Merubah include/config.php

```
Debian:~#vim /usr/share/cacti/site/include/config.php
```

Cari bagian-bagian ini dan tambahkan user, password, database buat di cacti

1. \$database_default = "cacti";
2. \$database_hostname = "localhost";

```
$database_username = "cactiuser";
```

```
$database_password = "cacti";
```

Ubah permissions directory-nya

```
Debian:~#chown -R cactiuser /usr/share/cacti/site/rra
```

```
Debian:~#chown -R cactiuser /usr/share/cacti/site/log
```

Merubah `/etc/crontab`

```
Debian:~#vim /etc/crontab
```

Masukan baris berikut ini

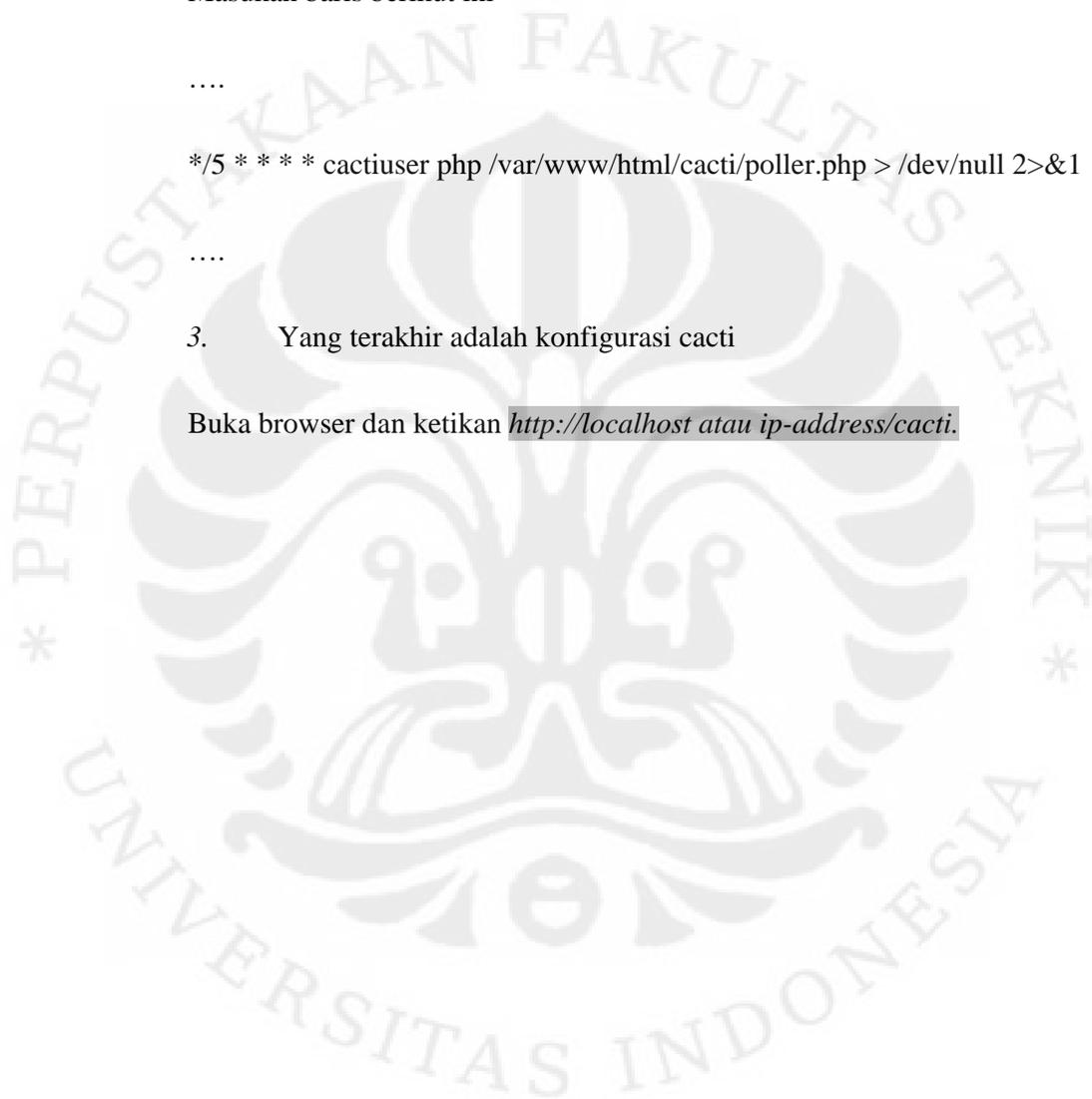
....

```
*/* * * * * cactiuser php /var/www/html/cacti/poller.php > /dev/null 2>&1
```

....

3. Yang terakhir adalah konfigurasi cacti

Buka browser dan ketikkan `http://localhost atau ip-address/cacti`.



Berikut ini adalah langkah konfigurasi QoS pada switch menjadi kelas tiga.

```
CSS-2950T-kedua(config)#access-list 3 permit host 192.168.1.4
CSS-2950T-kedua(config)#class-map ipclass3
CSS-2950T-kedua(config-cmap)#match access-group 3
CSS-2950T-kedua(config-cmap)#exit
CSS-2950T-kedua(config)#policy-map flow3t
CSS-2950T-kedua(config-pmap)#class ipclass3
CSS-2950T-kedu(config-pmap-c)#set ip dscp 24
CSS-2950T-kedu(config-pmap-c)#exit
CSS-2950T-kedua(config-pmap)#exit
CSS-2950T-kedua(config)#int fa0/3
CSS-2950T-kedua(config-if)#service-policy input flow3t
CSS-2950T-kedua(config-if)#end
```

Berikut ini adalah cara setting switch untuk mengklasifikasikan IP 192.168.1.4 kedalam QoS kelas lima.

```
CSS-2950T-kedua(config)#access-list 5 permit host 192.168.1.4
CSS-2950T-kedua(config)#class-map ipclass5
CSS-2950T-kedua(config-cmap)#match access-group 5
CSS-2950T-kedua(config-cmap)#exit
CSS-2950T-kedua(config)#policy-map flow5t
CSS-2950T-kedua(config-pmap)#class ipclass5
CSS-2950T-kedu(config-pmap-c)#set ip dscp 40
CSS-2950T-kedu(config-pmap-c)#exit
CSS-2950T-kedua(config-pmap)#exit
CSS-2950T-kedua(config)#int fa0/3
CSS-2950T-kedua(config-if)#service-policy input flow5t
CSS-2950T-kedua(config-if)#end
```

Langkah Konfigurasi Video Conference kelas 5 aplikasi yang lainnya kelas 1 dan 3

```
CSS-2950T-kedua(config)#access-list 1 permit host 192.168.1.3
```

```
CSS-2950T-kedua(config)#access-list 3 permit host 192.168.1.2
```

```
CSS-2950T-kedua(config)#access-list 5 permit host 192.168.1.4
```

```
CSS-2950T-kedua(config)#class-map ipclass1
```

```
CSS-2950T-kedua(config-cmap)#match access-group 1
```

```
CSS-2950T-kedua(config-cmap)#exit
```

```
CSS-2950T-kedua(config)#class-map ipclass3
```

```
CSS-2950T-kedua(config-cmap)#match access-group 3
```

```
CSS-2950T-kedua(config-cmap)#exit
```

```
CSS-2950T-kedua(config)#class-map ipclass5
```

```
CSS-2950T-kedua(config-cmap)#match access-group 5
```

```
CSS-2950T-kedua(config-cmap)#exit
```

```
CSS-2950T-kedua(config)#policy-map flow1t
```

```
CSS-2950T-kedua(config-pmap)#class ipclass1
```

```
CSS-2950T-kedu(config-pmap-c)#set ip dscp 8
```

```
CSS-2950T-kedu(config-pmap-c)#exit
```

```
CSS-2950T-kedua(config-pmap)#exit
```

```
CSS-2950T-kedua(config)#policy-map flow3t
```

```
CSS-2950T-kedua(config-pmap)#class ipclass3
```

```
CSS-2950T-kedu(config-pmap-c)#set ip dscp 24
```

```
CSS-2950T-kedu(config-pmap-c)#exit
```

```
CSS-2950T-kedua(config-pmap)#exit
```

```
CSS-2950T-kedua(config)#policy-map flow5t
```

```
CSS-2950T-kedua(config-pmap)#class ipclass5
```

```
CSS-2950T-kedu(config-pmap-c)#set ip dscp 40
```

```
CSS-2950T-kedu(config-pmap-c)#exit
```

```
CSS-2950T-kedua(config-pmap)#exit
```

```
CSS-2950T-kedua(config)#int fa0/1
```

```
CSS-2950T-kedua(config-if)#service-policy input flow3t
```

```
CSS-2950T-kedua(config-if)#exit
```

```
CSS-2950T-kedua(config)#int fa0/2
```

```
CSS-2950T-kedua(config-if)#service-policy input flow1t
```

```
CSS-2950T-kedua(config-if)#exit
```

```
CSS-2950T-kedua(config)#int fa0/3
```

```
CSS-2950T-kedua(config-if)#service-policy input flow5t
```

```
CSS-2950T-kedua(config-if)#exit
```

Berikut ini konfigurasi switch catalyst untuk video conference (Vicon) tidak diklasifikasikan, Packet Generator (PG) kelas tiga, dan website kelas satu (uji coba yang terakhir)

```
CSS-2950T-kedua(config)#access-list 1 permit host 192.168.1.3
```

```
CSS-2950T-kedua(config)#access-list 3 permit host 192.168.1.2
```

```
CSS-2950T-kedua(config-cmap)#match access-group 1
```

```
CSS-2950T-kedua(config-cmap)#exit
```

```
CSS-2950T-kedua(config)#class-map ipclass3
```

```
CSS-2950T-kedua(config-cmap)#match access-group 3
```

```
CSS-2950T-kedua(config-cmap)#exit
```

```
CSS-2950T-kedua(config)#policy-map flow1t
```

```
CSS-2950T-kedua(config-pmap)#class ipclass1
```

```
CSS-2950T-kedu(config-pmap-c)#set ip dscp 8
```

```
CSS-2950T-kedu(config-pmap-c)#exit
```

```
CSS-2950T-kedua(config-pmap)#exit
```

```
CSS-2950T-kedua(config)#policy-map flow3t
```

```
CSS-2950T-kedua(config-pmap)#class ipclass3
```

```
CSS-2950T-kedu(config-pmap-c)#set ip dscp 24
```

```
CSS-2950T-kedu(config-pmap-c)#exit
```

```
CSS-2950T-kedua(config-pmap)#exit
```

```
CSS-2950T-kedua(config)#int fa0/1
```

```
CSS-2950T-kedua(config-if)#service-policy input flow3t
```

```
CSS-2950T-kedua(config-if)#exit
```

```
CSS-2950T-kedua(config)#int fa0/2
```

CSS-2950T-kedua(config-if)#service-policy input flow1t

CSS-2950T-kedua(config-if)#end



Lampiran 2. Tabel Hasil Penelitian

TABEL HASIL PENGUKURAN *PACKET LOSS*

<i>Tabel Packet loss</i>	Paket Generator UDP	Packet Generator TCP
Sebelum implementasi QoS	0	1
video conference kelas 1	0	0
video conference kelas 3	0	0
video conference kelas 5	0	0
Aplikasi lain kelas 5& 3, vicon kelas 1	3741	4555
Aplikasi lain kelas 5 & 3, vicon tidak didefinisikan kelas	1425	2274

Keterangan
4555 dari 17831
3741 dari 18451
2274 dari 17605
1425 dari 16733

TABEL HASIL PENGUKURAN *DELAY*

Nilai Delay	Paket Generator UDP (ms)	Packet Generator TCP (ms)
Sebelum implementasi QoS	43	9
video conference kelas 1	32	33
video conference kelas 3	23	22
vicon conference 5	40	11
Aplikasi lain kelas 3&5 , vicon kelas 1	7086	2028
Aplikasi lain kelas 3 & 5, vicon tidak didefinisikankelas	13120	25

TABEL HASIL PENGUKURAN THROUGHPUT

Nilai Throughput <i>endpoint</i> pertama	Paket Generator UDP (Mbps)	Packet Generator TCP (Mbps)
Sebelum implementasi QoS	0.391	0.512
vicon kelas 1	0.53	0.459
vicon kelas 3	0.555	0.545
vicon kelas 5	0.563	0.594
Aplikasi lain kelas 5 & 3, vicon kelas 1	0.511	0.564
Aplikasi lain kelas 5 & 3	0.462	0.538

Nilai Throughput <i>endpoint</i> kedua	Paket Generator UDP (Mbps)	Packet Generator TCP (Mbps)
Sebelum implementasi QoS	0.391	0.512
vicon kelas 1	0.53	0.459
vicon kelas 3	0.555	0.545
vicon kelas 5	0.563	0.594
Aplikasi lain kelas 5 & 3, vicon kelas 1	0.536	0.555
Aplikasi lain kelas 5 & 3	0.492	0.545

TABEL HASIL PENGUKURAN JITTER.

Tabel 1 Sebelum implementasi QoS pada endpoint pertama

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	16.71	8.32
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	14.93	4.45
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	16.63	8.08
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	13.02	5.11
Mean jitter dan Jumlah Paket							6.49

Tabel 2 Sebelum implementasi QoS pada endpoint kedua

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	22.19	19.92
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	17.21	1.36
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	21.7	19.86
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	11.07	1.3
Mean jitter dan Jumlah Paket							10.61

Tabel 3 Video Conference kelas 1 pada endpoint pertama

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	12.89	7.18
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	10.73	4.19
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	16.66	8.42
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	17.54	4.35
Mean jitter dan Jumlah Paket							6.035

Tabel 4 Video Conference kelas 1 pada endpoint kedua

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590		21.86	19.49
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	10.94	0.9
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	21.75	19.51
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	20.92	0.94
Mean jitter dan Jumlah Paket							10.21

Tabel 5 Video Conference kelas 3 pada endpoint pertama

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	15.45	8.64
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	15.99	1.41
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	16.47	8.78
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	7.02	1.43
Mean jitter dan Jumlah Paket							5.065

Tabel 6 Video Conference kelas 3 pada endpoint kedua

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	21.73	19.33
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	21.15	1.01
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	22.39	19.34
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	8.14	1
Mean jitter dan Jumlah Paket							10.17

Tabel 7 Video Conference kelas 5 pada endpoint pertama

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	17.23	9.5
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	11.1	1.36
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	16.81	8.66
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	7.64	1.41
Mean jitter dan Jumlah Paket							5.2325

Tabel 8 Video Conference kelas 5 pada endpoint kedua

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	22.07	19.86
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	11.27	0.87
UDP	192.168.1.6	49594	192.168.1.8	49594	H.263	21.99	17.76
UDP	192.168.1.8	49596	192.168.1.6	49596	G.723	8.68	0.96
Mean jitter dan Jumlah Paket							9.8625

Tabel 9 Video conference kelas 1, aplikasi lain kelas 3&5 pada endpoint pertama

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	16.25	8.76
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	1.85	2.13
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	17.17	7.58
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	12816.99	24.36
Mean jitter dan Jumlah Paket							10.7075

Tabel 10 Video conference kelas 1, aplikasi lain kelas 3&5 pada endpoint kedua

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	21.71	19.57
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	15.04	0.78
UDP	192.168.1.6	49594	192.168.1.8	49590	H.263	22.55	19.22
UDP	192.168.1.8	49596	192.168.1.6	49592	G.723	16.66	0.94
Mean jitter dan Jumlah Paket							10.1275

Tabel 11 Vicon tidak diklasifikasikan, aplikasi lain kelas 1&3 endpoint pertama

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	7400.86	6.02
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	16.97	8.66
UDP	192.168.1.6	49594	192.168.1.8	49594	H.263	16.32	8.28
UDP	192.168.1.8	49596	192.168.1.6	49596	G.723	2963.02	14.39
Mean jitter dan Jumlah Paket							9.3375

Tabel 12 Vicon tidak diklasifikasikan, aplikasi lain kelas 5&3 endpoint kedua

PG	Asal IP	Asal Port	Tujuan IP	Tujuan Port	Payload	Max Jitter	Mean Jitter
TCP	192.168.1.6	49590	192.168.1.8	49590	H.263	15.23	2.66
TCP	192.168.1.8	49592	192.168.1.6	49592	G.723	22.72	19.44
UDP	192.168.1.6	49594	192.168.1.8	49594	H.263	21.56	19.71
UDP	192.168.1.8	49596	192.168.1.6	49596	G.723	21.51	0.94
Mean jitter dan Jumlah Paket							10.6875