

**ANALISIS PERBANDINGAN PERFORMA PROTOKOL RTP DAN SRTP
PADA APLIKASI VOIP**

TUGAS AKHIR

**Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika**



Oleh :

Nama: Umar Sami

NIM: 06 523 019

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA**

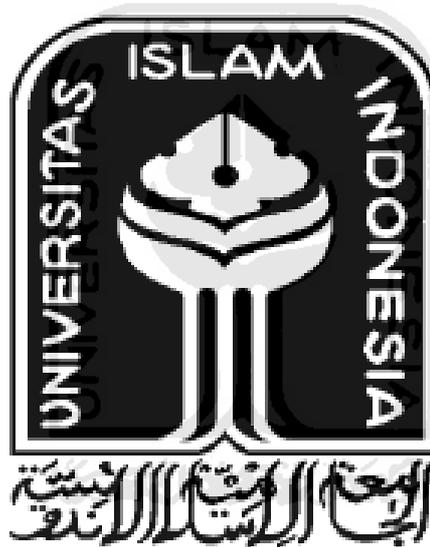
2011

HALAMAN JUDUL

**ANALISIS PERBANDINGAN PERFORMA PROTOKOL RTP DAN SRTP
PADA APLIKASI VOIP**

TUGAS AKHIR

**Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika**



Oleh :

Nama: Umar Sami

NIM: 06 523 019

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA**

2011

**LEMBAR PENGESAHAN PEMBIMBING
ANALISIS PERBANDINGAN PERFORMA PROTOKOL RTP DAN SRTP
PADA APLIKASI VOIP**



Oleh :

Oleh :

Nama: Umar Sami

NIM: 06 523 019

Yogyakarta, 18 Juli 2011

Pembimbing

(R. Teduh Dirgahayu, ST., M.Sc.)

LEMBAR PENGESAHAN PENGUJI
ANALISIS PERBANDINGAN PERFORMA PROTOKOL RTP DAN SRTP
PADA APLIKASI VOIP

TUGAS AKHIR

oleh:

Nama : Umar Sami

No Mahasiswa : 06 523 019

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, tanggal bulan 2011

Tim Penguji

R. Teduh Dirgahayu, ST., M.Sc

Ketua

Hendrik ST., M.Eng.

Anggota I

Syarif Hidayat S.Kom., MIT.

Anggota II

Mengetahui,

Ketua Jurusan Teknik Informatika

Universitas Islam Indonesia



(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Umar Sami

NIM : 06 523 019

Menyatakan bahwa seluruh komponen dan isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini bukan merupakan hasil karya saya sendiri, maka saya siap menanggung resiko dan konsekuen apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 18 Juli 2011

(Umar Sami)

HALAMAN PERSEMBAHAN

*Ayah dan Ibu tersayang.. karya kecil ini sebagai tanda baktiku
untukmu..*



*Untuk agamaku, bangsaku, dan para insan IS
semoga karya ini bermanfaat..*

MOTTO

“.... sesungguhnya setelah kesulitan tersimpan sebuah kemudahan “

(QS. Al Insiroh :6)

“Sesungguhnya sesudah kesulitan itu ada kemudahan ; Maka apabila kamu telah selesai (dari suatu urusan), kerjakanlah dengan sungguh-sungguh (urusan) yang lain ”.



(Q.S. Alama Nasyrah ayat 6 dan 7)

KATA PENGANTAR

Assalaamu'alaikum warahmatullahi wabarakaatuh

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya kepada penulis sehingga penulis dapat menyelesaikan penyusunan Laporan Tugas Akhir ini dengan baik. Sholawat serta salam penulis curahkan kepada Nabi Besar Muhammad SAW yang penulis tunggu syafaatnya di hari akhir.

Laporan Tugas Akhir ini dibuat sebagai salah satu syarat yang harus dipenuhi untuk memperoleh gelar sarjana di Jurusan Teknik Informatika, Fakultas Teknologi Industri Universitas Islam Indonesia.

Penulis menyadari bahwa selama penyusunan laporan tugas akhir ini tidak terlepas dari bantuan, bimbingan, dan dukungan baik secara material maupun moral dari berbagai pihak. Oleh karena itu penulis mengucapkan banyak terima kasih kepada:

1. Allah SWT atas segala karunia, rahmat dan hidayahNya, juga kepada junjungan kita Nabi besar Muhammad SAW
2. Kedua orangtuaku atas segala limpahan cinta,kasih sayang,doa,dan dukungan yang tiada henti dan tidak akan pernah berhenti.
3. Bapak Gumbolo Hadi Susanto, Ir., M.Sc selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Yudi Prayudi, S.Si., M.Kom., selaku Ketua Jurusan Teknik Informatika Fakultas Teknologi Industri.
5. Bapak R. Teduh Dirgahayu, ST., M.Sc., selaku dosen pembimbing tugas akhir penulis. Terima kasih atas segala bimbingan, dukungan dan masukan yang

telah diberikan kepada penulis sehingga penyusunan laporan tugas akhir ini dapat terselesaikan dengan baik.

6. Bapak R. Ranta Dewa, selaku dosen jaringan komputer yang telah mengenalkan dunia jaringan dengan penuh kesabaran.
7. Bapak Azmiansyah, S.T., selaku dosen jaringan komputer yang telah mengarahkan dan membimbing penulis dalam membangun server Voice Over Internet Protocol.
8. Bapak Onno W.Purbo, dan kawan-kawan forum kios yang telah memberikan bimbingannya walau hanya lewat dunia maya.
9. Teman-teman FIRE dan seluruh teman-teman Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia. Terima kasih atas dukungannya kepada penulis.
10. Para penghuni Asrama Putra Amanah, Abdullah Sulaiman Maretan –Tetep teges!, Saleh Bafadal –Orang paling romantis se-Bondowoso, Rayyan Muchamad Maretan – Jiron Kamil, syukran katsir ya akh, Hafid Ali Kelib – nyripit gahwa sitik ya fid=D, Jamal Ali Kelib –klo bikin pancake sami nya di ajak ya mal, Ikrimah Abbad – sukran atas saran dan kritiknya ya pak =D.
11. Untuk para mantan “Penghuni Jalur Gaza” Robiq Shammakh, Hanif Hatrash, Salim Shammakh, terima kasih atas kenangan dan pelajaran di padepokan dunia hitam persilatan.
12. Pemuda Al-irsyad cabang Jogjakarta, yang telah memberikan pelajaran berharga tentang kehidupan, tentang organisasi, tentang tanggung jawab, agama dan segalanya. Mari perdengarkan raum Jogja lagi demi kebaikan bersama, demi Jogjakarta.
13. Seluruh teman-teman dan barbagai pihak yang telah membantu baik secara langsung maupun tidak langsung kepada penulis.

Tidak lepas dari segala kekurangan, penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini mengingat keterbatasan waktu dan pengetahuan yang penulis miliki. Karena itu segala kritik dan saran yang bersifat membangun dari pembaca sekalian sangat penulis harapkan demi kesempurnaan laporan ini.

Besar harapan penulis semoga laporan tugas akhir ini dapat memberikan manfaat bagi penulis khususnya dan bagi para pembaca sekalian.

Wassalaamu'alaikum warahmatullahi wabarakaatuh.



Yogyakarta, 18 Juli 2011

Penulis

Umar Sami

ABSTRAKSI

Teknologi telekomunikasi saat ini berkembang pesat. Salah satu solusi komunikasi murah jarak jauh adalah VoIP (*Voice over Internet Protocol*). VoIP adalah sebuah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet protocol. VoIP menggunakan protokol UDP, protokol tersebut adalah SIP (*Session Initiation Protocol*) untuk signalling dan RTP (*Real-Time Transport Protocol*) untuk membawa data suara ketika terjadi percakapan suara. Seperti halnya teknologi komunikasi yang lain, VoIP juga memiliki metode pengamanan, salah satunya menggunakan protokol SRTP (*Secure Real-time Transport Protocol*). Protokol ini mengamankan pengiriman percakapan suara dengan melakukan enkripsi pada bagian pembawa data suara atau disebut *payload*.

Dengan menggunakan SRTP keamanan akan terjamin, tetapi kualitas performa akan mengalami penurunan karena paket yang dikirimkan lebih besar daripada RTP. Parameter yang digunakan untuk melakukan penilaian perbedaan adalah delay, jitter, dan packet loss. perbedaan nilai delay antara RTP dan SRTP adalah sebesar 200%, jitter sebesar 4%, dan packet loss 0%. Hal ini terjadi karena pada SRTP memiliki bagian tambahan untuk enkripsi, dan mengalami proses enkripsi dan dekripsi.

Keyword: RTP, SRTP, Delay, Jitter, Paket loss.

TAKARIR

<i>Quality of Service</i>	Kualitas layanan
<i>IP Telephony</i>	Telepon berbasis Internet Protokol
<i>Packet-switch</i>	Pertukaran paket data
<i>IP- Private Branch Exchange</i>	Perangkat server yang mengendalikan alur masuk dan keluar panggilan telepon berbasis Internet Protocol.
<i>Uniform Resource Identification</i>	Kesatuan karakter yang digunakan untuk identifikasi nama atau sumber daya dari dan ke internet.



DAFTAR ISI

HALAMAN JUDUL	ii
LEMBAR PENGESAHAN PEMBIMBING	iii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR.....	v
HALAMAN PERSEMBAHAN	vi
MOTTO	vii
KATA PENGANTAR.....	viii
ABSTRAKSI.....	xi
TAKARIR.....	xii
DAFTAR ISI.....	xiii
DAFTAR GAMBAR.....	xvi
DAFTAR TABEL	xvii
BAB I 1	
PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Penelitian.....	3
1.7 Studi Pustaka	3
1.8 Implementasi Perangkat Lunak	3
1.9 Sistematika Penulisan.....	4

BAB II 6

LANDASAN TEORI.....	6
2.1 Voice Over Internet Protocol.....	6
2.1.1 Protokol – Protokol VoIP.....	8
2.2 PBX (Internet Protocol Private Branch Exchange).....	17
2.3 SRTP (Secure Real Time Protocol).....	18
2.3.1 Susunan SRTP.....	19
2.3.2 LibSRTP.....	20
2.4 QoS (Quality of Service).....	20

BAB III 22

METODOLOGI.....	22
3.1 Analisis Masalah.....	22
3.2 Implementasi sistem.....	23
3.2.1 Kebutuhan Perangkat Lunak.....	23
3.2.2 Kebutuhan Perangkat Keras.....	24
3.3 Topologi.....	25
3.4 Konfigurasi.....	25
3.4.1 Konfigurasi server.....	25
3.4.2 Konfigurasi klien.....	27
3.5 Rencana Pengujian.....	32

BAB IV 34

HASIL DAN PEMBAHASAN.....	34
4.1 Hasil dan Pembahasan Protokol RTP dan SRTP.....	34
4.2 Perbandingan Hasil Pengamatan.....	36

BAB V 43

KESIMPULAN DAN SARAN	43
5.1 Kesimpulan.....	43
5.2 Saran	43



DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi susunan TCP/IP protocol.....	8
Gambar 2. 2 Skema RTP <i>Header</i>	11
Gambar 2. 3 Skema Topologi SIP server.....	13
Gambar 2. 4 Gambar komunikasi SIP.....	15
Gambar 2. 5 Gambar skema SRTP <i>header</i>	19
Gambar 3. 1 Gambaran umum implementasi VoIP	22
Gambar 3. 2 Gambar topologi jaringan.....	25
Gambar 3. 3 Pendaftaran SIP <i>Account</i>	28
Gambar 3. 4 Pemberian SIP Account	28
Gambar 3. 5 Pemilihan metode penggunaan enkripsi	29
Gambar 3. 6 Gambar pemilihan <i>interface</i>	30
Gambar 3. 7 Gambar VoIP Calls	30
Gambar 3. 8 Gambar grafik SIP dan RTP <i>player</i>	31
Gambar 3. 9 Gambar halaman VQManager	32
Gambar 3. 10 Gambar <i>monitoring Delay, Jitter dan Packet Loss</i>	32

DAFTAR TABEL

Tabel 3. 1 Konfigurasi alamat IP	26
Tabel 3. 2 Konfigurasi pada sip.conf	26
Tabel 3. 3 Konfigurasi extensions.conf.	27
Tabel 4. 1 hasil rata-rata perhitungan RTP dan SRTP dengan bandwidh 64kb. .	38
Tabel 4. 2 Hasil rata-rata perhitungan RTP dan SRTP dengan bandwidh 128kb.	38
Tabel 4. 3 Hasil rata-rata perhitungan RTP dan SRTP dengan bandwidh 512kb.	39
Tabel 4. 4 Hasil rata-rata perhitungan RTP dan SRTP dengan bandwidh 1Mb. .	39
Tabel 4. 5 Perbandingan delay antara RTP dan SRTP dengan variasi bandwid. .	40
Tabel 4. 6 Perbandingan jitter antara RTP dan SRTP dengan variasi bandwid. .	40
Tabel 4. 7 Perbandingan paket loss antara RTP dan SRTP dengan variasi bandwid.....	40

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini teknologi komunikasi sudah berkembang pesat. Salah satu teknologi yang saat ini mulai ramai digunakan adalah VoIP. VoIP adalah kependekan dari *Voice over Internet Protocol*, yaitu sebuah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet. Dari segi keamanan, VoIP sama halnya dengan transmisi data konvensional, yakni tetap rawan dengan serangan-serangan keamanan.

Keamanan suatu jaringan komputer adalah hal yang sangat sensitif dalam teknologi komunikasi. Teknik-teknik dan metoda-metoda pengamanan banyak dikembangkan dalam teknologi komunikasi menilik kepentingan data yang ada dalam setiap paket yang di transmisikan. Salah satu metode keamanan salam VoIP adalah dengan menggunakan SRTP, yang mana teknologi ini melakukan pengamanan dengan enkripsi pada protokol RTP yang membawa data suara. Kualitas keamanan VoIP menjadi topik yang hangat di perbincangkan baik antara praktisi jaringan atau bagi para pengguna, namun di lain sisi kualitas suara sebuah jaringan VoIP juga menjadi pilihan utama, jangan sampai dengan metode keamanan yang diterapkan kualitas suara menjadi buruk sehingga jaringan VoIP yang digunakan tetap aman dan kualitas suara tetap terjamin.

Salah satu bagian dari VoIP adalah paket data yang membawa data atau suara yang dikirimkan saat menggunakan layanan VoIP. Bagian ini menjadi rawan penyerangan, baik penyerangan yang merusak ataupun dengan penyadapan. Untuk menghindari agar penyadapan tidak terbaca oleh penyerang maka salah satu cara yang digunakan adalah dengan metode pengamanan enkripsi data. Namun secara logika, penerapan enkripsi pada paket data akan berdampak pada

pembesaran ukuran paket data tersebut yang mungkin akan mengganggu atau mengurangi kualitas dari layanan VoIP tersebut.

1.2 Perumusan Masalah

Kemanan merupakan masalah yang penting bagi seorang teknisi jaringan komputer di lain sisi para pengguna layanan menginginkan kualitas suara dan layanan yang optimal dalam penggunaan layanan VoIP. Hal ini bersifat berbanding terbalik dan inilah yang menjadi daya tarik pembahasan.

1. Bagaimana mengukur kualitas layanan VoIP dari sisi paket data terhadap faktor metoda-metoda kemanan yang diterapkan.
2. Apakah metoda keamanan paket data yang diterapkan merupakan layanan yang baik namun tetap aman.
3. Bagaimanakah perbandingan QoS antara RTP dengan SRTP.

1.3 Batasan Masalah

Batasan masalah yang diangkat oleh penulis dalam penelitian ini adalah:

1. Protokol tranport media pada aplikasi VoIP saja.
2. Metode pengamanan hanya pada protokol SRTP saja dengan menghiraukan metode pengamanan jaringan.
3. Membatasi penggunaan VoIP hanya dalam lingkup jaringan lokal.
4. Tanpa melakukan uji penetrasi terhadap metode keamanan yang digunakan.
5. Membatasi parameter penilaian performa dengan delay jitter dan packet loss

1.4 Tujuan Penelitian

Tujuan penelitian adalah untuk membandingkan layanan metode enkripsi yang diterapkan pada jaringan VoIP dalam pengiriman data, sehingga ditemukan metode keamanan dengan QoS (*Quality of Service*) yang baik.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah didapatkannya metode enkripsi yang terbaik yang dapat digunakan dalam pengiriman data dalam jaringan VoIP sehingga mendapatkan nilai kualitas yang terbaik.

1.6 Metode Penelitian

Untuk memenuhi tujuan yang akan dicapai melalui penulisan skripsi ini, maka ada beberapa metode yang akan digunakan, yaitu:

1. Studi literatur dari buku – buku, makalah, ataupun manual – manual dan berbagai sumber online lainnya.
2. Implementasi VoIP menggunakan protokol RTP dan SRTP.
3. Ujicoba performa bertujuan untuk mengamati perbandingan performa RTP dan SRTP.

1.7 Studi Pustaka

Pada penelitian ini peneliti mengawali dengan studi pustaka dari buku-buku literatur dan dari tugas akhir yang berkaitan dengan penelitian.

Peneliti juga mengambil beberapa artikel dan informasi-informasi yang dianggap perlu dari Internet untuk mendukung penelitian, seperti kebutuhan perangkat keras, perangkat lunak, arsitektur dan informasi-informasi lainnya yang di anggap perlu dalam implementasi penelitian QoS data VoIP.

1.8 Implementasi Perangkat Lunak

Implementasi penelitian berdasarkan pengumpulan informasi dan literatur yang meliputi :

1. Desain Arsitektur Jaringan dan Alokasi Account

Tahap ini merupakan tahap perancangan arsitektur jaringan komputer yang akan digunakan untuk membangun VoIP SRTP serta pengalokasian account dan penyusunan pengendalian telpon atau biasa disebut *dial plan*.

2. Pengadaan perangkat keras

Tahapan ini merupakan tahap pengadaan perangkat keras untuk server dan client VoIP SRTP. Selain itu diperlukan pula perangkat keras yang digunakan sebagai pendukung keberlangsungan transmisi data suara, antara lain seperangkat PC sebagai server dan minimalnya dua buah PC/laptop sebagai client dengan aplikasi softphone didalamnya.

3. Instalasi dan konfigurasi perangkat lunak

Tahapan ini merupakan tahap instalasi software pada komputer server dan client VoIP SRTP. Kemudian dilanjutkan dengan mengkonfigurasi software pada server dan client VoIP SRTP.

4. Pengujian

Setelah konfigurasi selesai dilakukan, tahapan selanjutnya adalah pengujian QoS dari arsitektur dan konfigurasi yang telah dibangun. Pada tahap ini dilakukan pembacaan kualitas dari transfer data dari jaringan yang telah dibangun dengan menggunakan beberapa aplikasi pendukung seperti wireshark, dan VQ Manager.

1.9 Sistematika Penulisan

Sistematika ini digunakan dalam penyusunan laporan tugas akhir ini adalah sebagai berikut :

Bab I Pendahuluan

Pada bab ini dikemukakan latar belakang permasalahan, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penelitian.

Bab II Landasan Teori

Pada bab ini akan dibahas teori yang mendasari dalam pengujian dampak enkripsi paket VoIP terhadap *Quality of Service*.

Bab III Metodologi

Bab ini memuat uraian tentang metode analisis, analisis masalah dan hasil analisis yang mencakup kebutuhan perangkat keras dan lunak, gambaran umum sistem, analisis kebutuhan sistem, arsitektur jaringan dan rancangan aliran data ketika dilakukan panggilan.

Bab IV Hasil dan Pembahasan

Pada bab ini akan dibahas implementasi pembangunan VoIP SRTP dan analisa hasil uji coba dengan menggunakan tool-tool yang telah di tentukan.

Bab V Penutup

Bab ini memuat kesimpulan-kesimpulan dari seluruh rangkaian proses implementasi perangkat lunak, baik pada tahap analisis, perancangan, implementasi, terutama pada analisis kerja aplikasi. Bab ini juga membahas saran yang digunakan oleh pihak yang berkepentingan maupun untuk peneliti terhadap kekurangan serta keterbatasan dalam penelitian ini.

BAB II

LANDASAN TEORI

2.1 Voice Over Internet Protocol

Voice Over Internet Protocol (VoIP) dikenal juga dengan sebutan *IP telephony*. VoIP didefinisikan sebagai suatu sistem yang menggunakan jaringan untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP. Iskandariyah (Iskandariyah,2003) menyebutkan bahwa VoIP merupakan teknologi yang mampu melewati trafik suara, video, dan data yang berbentuk paket melalui jaringan IP. Jaringan IP sendiri merupakan jaringan komunikasi data yang berbasis *packet-switch* [OWP07].

Salah satu bagian utama arsitektur VoIP adalah PBX (*Private Branch Exchange*) yang berlaku sebagai server penghubung antara pengguna aplikasi VoIP *client/softphone* ataupun ke layanan PSTN. Salah satu aplikasi open source yang dapat digunakan adalah Asterisk. Di dalamnya terdapat protokol yang dapat mengirimkan data secara *realtime* (waktu nyata). Protokol ini bernama RTP (*Real Time Protokol*). RTP melewati data dalam jaringan tanpa dienkripsi yang dapat dengan mudah dibaca oleh pihak lain yang tidak berwenang. Untuk mengamankan data tersebut, dibuatlah protokol SRTP (*Secure Real Time Protokol*)

Protokol tersebut digunakan dalam berbagai layanan multimedia sebagai alternatif dari teknologi komunikasi pendahulunya. Layanan tersebut antara lain

1. Layanan telepon dengan biaya yang lebih terjangkau karena menggunakan jaringan Internet, sehingga tidak perlu membangun infrastruktur jaringan baru.
2. Layanan *voice message* yang dapat ditinggalkan pada nomor yang dihubungi.

3. Layanan faksimili dengan biaya yang terjangkau.
4. Layanan *video chat* atau *video conferencing* di mana dua orang atau lebih dapat berbincang dengan teks atau suara dengan menampilkan video lawan bicaranya.

Dalam komunikasi VoIP memiliki parameter tertentu untuk melakukan penilaian performa agar dapat memenuhi standar kualitas. Parameter tersebut adalah:

1. Delay

Dalam perancangan jaringan VoIP, delay merupakan suatu permasalahan yang harus diperhitungkan karena kualitas bagus tidaknya suara tergantung dari waktu delay. Besarnya delay maksimum yang direkomendasikan oleh ITU untuk aplikasi suara adalah 150 ms, sedangkan delay maksimum dengan kualitas suara yang masih dapat diterima pengguna adalah 250 ms

2. Jitter

Jitter merupakan variasi dari delay. Jitter dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan. Pengaruh jitter pada kinerja jaringan harus dilihat bersama delay. Ketika jitter besar namun *delay*-nya kecil maka kinerja jaringan tidak bisa dikatakan jelek karena besarnya jitter dapat dikompensasi dengan nilai delay yang kecil. Jitter akan menurunkan kinerja jaringan ketika nilainya besar dan juga nilai delay-nya juga besar.

3. Paket loss

Merupakan suatu keadaan dimana suatu paket tidak sampai ke tujuan atau gagal ke tujuan .

2.1.1 Protokol – Protokol VoIP

Didalam dunia komunikasi komputer diperlukan beberapa perangkat jaringan agar dapat saling berkomunikasi. Pengalamatan pada tiap perangkat juga dilakukan agar setiap paket dapat dikirimkan ke tujuan yang benar. Protokol digunakan sebagai penerjemah dalam telekomunikasi komputer. Dalam jaringan komputer terdapat berbagai macam protokol, akan tetapi di perlukan protokol yang sama agar kedua komputer dapat berkomunikasi dengan baik.

6. Protokol TCP/IP

TCP/IP (*Transfer Control protocol/Internet Protocol*) merupakan suatu protocol yang digunakan pada jaringan. Gambar 2.1 adalah ilustrasi susunan protokol TCP/IP

Application	Application
Transport	Transport
Internetwork	Internetwork
Physical	Physical

Gambar 2. 1 Ilustrasi susunan TCP/IP protocol

A. *Application Layer*

Application layer atau lapisan aplikasi berfungsi sebagai pengirim file dari sebuah system ke system yang berbeda agar file tersebut sampai dengan baik dan dapat digunakan sebagaimana mestinya. Lapisan ini berhubungan dengan protokol yang digunakan sebagai dasar. Contoh protokol aplikasi yang banyak dikenal adalah HTTP (*Hypertext transfer protocol*), FTP (*File Transfer Protocol*) untuk perpindahan file, dan TELNET untuk akses terminal jarak jauh .

B. *Transport Layer*

Terdapat dua jenis protokol dalam lapisan ini, yaitu TCP dan UDP.

TCP (*Transmission Control Protocol*) adalah protokol yang membangun koneksi antara dua titik ujung sistem dan koneksi ini akan selalu terjaga hingga pengiriman data selesai dengan sempurna. TCP bertugas memberikan informasi urutan paket ke setiap paket yang dikirimkan yang kemudian pada ujung satunya akan menyusun kembali paket-paket tersebut sehingga menjadi sebuah file kembali dan dapat digunakan sebagai mana mestinya.

UDP (*User Datagram Protocol*) adalah protokol yang digunakan IP untuk mengirimkan data satu komputer ke komputer lainnya. Berbeda dengan TCP, protokol UDP tidak memberikan informasi urutan pada paket-paket yang dikirimkannya. UDP tidak mengurutkan data, UDP hanya memastikan koneksi awal sudah terjadi lalu mengirimkan paketnya tanpa memastikan apakah paket tersebut sampai tujuan dalam urutan yang benar.

C. *Internetwork Layer*

Lapisan ini bertanggung jawab melakukan pemetaan jalur dan melakukan enkapsulasi paket-paket jaringan menjadi paket-paket IP. Protokol yang berjalan pada lapisan ini antara lain IP (*Internet Protocol*), IGMP (*Internet Group Management Protocol*), dan ICMP (*Internet Control Message Protocol*).

D. *Physical Layer*

Physical layer adalah lapisan terendah pada protokol TCP/IP. Lapisan ini meletakkan paket-paket data pada media perangkat keras antarmuka jaringan, LAN dengan ethernet atau WAN dengan modem dial-up pada jaringan telepon PSTN.

1. Protokol SIP (*Session Initiation Protocol*)

SIP adalah suatu *signaling protocol* pada lapisan aplikasi yang berfungsi untuk membangun, memodifikasi dan mengakhiri suatu sesi komunikasi multimedia. Sesi multimedia adalah suatu pertukaran data antara pengguna yang meliputi suara, video dan data atau text.

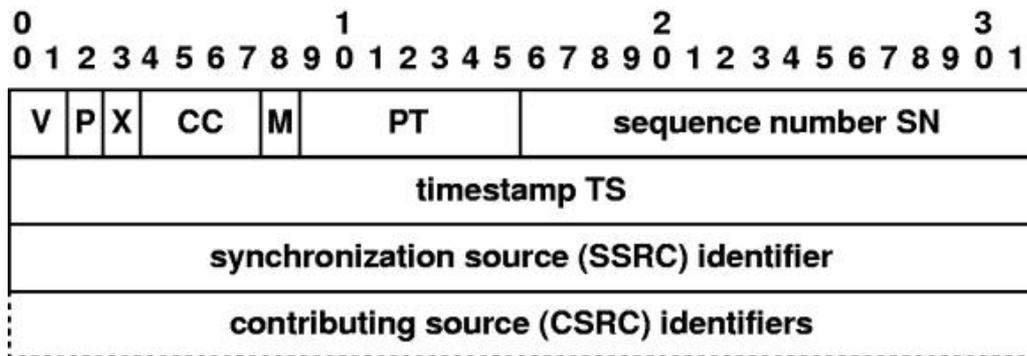
SIP tidak memberikan keterangan sesi apa yang dijalankan, namun hanya mengakomodasi sesi tersebut. Dengan fleksibilitas tersebut, SIP dapat digunakan oleh banyak aplikasi multimedia seperti game interaktif, musik dan video termasuk *voice*, video dan *web conferencing*.

1. Arsitektur SIP

SIP memiliki beberapa bagian pembentuk dalam paket protokol ini. Pada SIP terdapat protokol yg mendukung agar data terkirim *real-time*. [TJN10]

1. RTP (*Real-Time Transport Protocol*)

RTP adalah protokol untuk membebaskan *jitter* dan *desequencing* yang terjadi pada jaringan IP. RTP dapat digunakan untuk beberapa macam transfer data *real time* seperti video dan suara. RTP berisi tipe data yang dikirimkan, seperti *timestamps*, yang di gunakan sebagai pengatur waktu percakapan agar terdengar seperti yang di ucapkan dan *sequence number*. RTP dirancang untuk berjalan menggunakan UDP karena TCP tidak dapat menangani pengiriman data yang *real-time* dengan *delay* yang relatif kecil, seperti pada pengiriman data komunikasi suara. Dengan menggunakan UDP yang dapat mengirimkan paket IP secara *multicast*, RTP *stream* yang dibentuk oleh satu terminal dapat dikirimkan ke beberapa terminal tujuan. Skema paket RTP dapat dilihat pada gambar 2.2.



Gambar 2. 2 Skema RTP Header

2. RTCP (*Real-Time Transport Control Protocol*)

RTCP adalah protokol yang digunakan bersamaan dengan RTP. RTCP bertugas untuk mengirimkan paket kontrol setiap user yang berpartisipasi pada percakapan dan digunakan sebagai informasi kualitas transmisi pada jaringan.

RTCP memiliki fungsi utama sebagai pengirim laporan kualitas dan media control. RTCP memiliki informasi seperti paket yang hilang (*packet loss*), *jitter*, keterlambatan (*delay*), level sinyal, *Call Quality Metrics*, *Echo Return Loss*.

RTCP memiliki beberapa jenis packet yang berbeda:

3. *Sender Report* (SR)

Paket ini dikirim secara periodik oleh pengirim yg aktif dalam sesi untuk melaporkan pengiriman dan penerimaan untuk semua paket RTP yang dikirim selama interval sesi komunikasi.

4. *Receiver Report* (RR)

Paket ini ditujukan kepada user yang telah register tetapi tidak mengirimkan paket RTP. Laporan ini berisi kualitas layanan.

5. *Source Description* (SDES)

Pesan ini berisi tentang informasi seperti nama, alamat, email, nomor telepon dan alamat sumber paket berasal.

6. *End of participant* (BYE)

Pesan ini berisi informasi bahwa pengirim meninggalkan konferensi/*offline*.

7. *Application-specific message* (APP)

Pesan ini mengirimkan pesan unik dari aplikasi yang berfungsi untuk menyatakan desain ekstensi khusus protokol RTCP.

Selain RTP dan RTCP, SIP memiliki dua komponen penting yaitu User Agent dan Server.

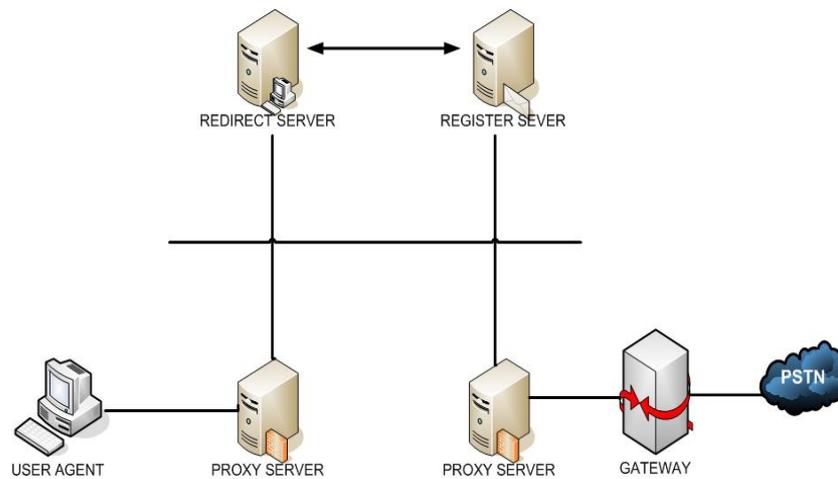
User Agent digunakan untuk memulai, menerima, dan mengakhiri sesi komunikasi. User Agent dibagi dua, yaitu:

1. *User Agent Service* (UAS), adalah bagian yang menerima dan menanggapi sesi komunikasi.
2. *User Agent Client* (UAC), adalah bagian yang memiliki sesi komunikasi.

Kedua jenis User Agent ini dapat menutup sesi komunikasi, dalam artian UAS dapat menutup sesi komunikasi meskipun UAC tidak menutup sesi komunikasi tersebut. User Agent ini dapat berupa *softphone* atau *IP-phone*.

Server digunakan untuk melayani permintaan (*request*) dari *client* dan memberikan tanggapan (*response*) atas permintaan yang dibuat.

Dalam SIP ada tiga buah server, sebagaimana dijelaskan dalam Gambar 2.3 berikut:



Gambar 2. 3 Skema Topologi SIP server

8. Proxy Server

Proxy Server merupakan penghubung antara user agent, yang bertugas menerima *request message* dari user agent pengirim kemudian meneruskan ke user agent penerima. *Request* dapat dilayani oleh proxy server sendiri atau disampaikan (*forward*) pada proxy server lain. Server ini juga menerjemahkan dan menulis ulang *request message* sebelum menyampaikannya pada user agent tujuan atau proxy lain. Fungsi dari proxy server adalah menyimpan seluruh keadaan (*state*) sesi komunikasi antar UAC dan UAS.

9. Redirect Server

Redirect server adalah komponen yang menerima *request message* dari user agent, memetakan alamat SIP user agent atau proxy server tujuan, kemudian menyampaikan hasil pemetaan kembali kepada user agent pengirim (UAC). Server ini tidak menyimpan keadaan sesi komunikasi antara UAC dan UAS setelah hasil pemetaan disampaikan kepada UAC. Tidak seperti proxy server, redirect server tidak dapat memulai inisiasi *request message* dan tidak seperti UAS, server ini tidak dapat menerima dan menutup sesi komunikasi

10. Register Server

Register server merupakan komponen yang menerima *request message REGISTER*, yaitu perintah mendaftarkan pesan yang akan dikirim. Register server dapat menambahkan fungsi otentikasi user untuk validasi. Server ini menyimpan database user untuk otentikasi dan lokasi sebenarnya (berupa alamat IP dan nomor port) agar user yang terdaftar dapat dihubungi oleh komponen SIP lainnya.

2. Pengalamatan SIP

Komunikasi pada SIP dilakukan dengan mengirimkan pesan yang berbasis HTTP. Pengalamatan dalam SIP dinyatakan dengan SIP-URI (*Uniform Resource Identification*). Format pengalamatan SIP ditunjukkan pada gambar 2.1

A rectangular box containing the text "[sip :] <username@ host>". The text is centered within the box. The box is overlaid on a faint watermark of the University of Indonesia logo.

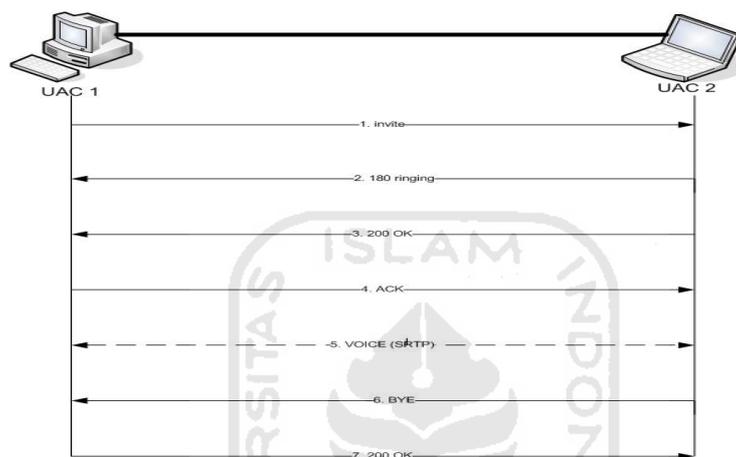
Gambar 2.1 Pengalamatan SIP

Contoh :

1. sip:samiy@192.168.1.2
2. sip:900@voiprakyat.or.id

3. Operasi Dasar SIP

Hubungan yang dibangun oleh SIP pada proses *signalling* bersifat *client/server*. Dengan demikian ada 2 jenis message, yaitu *request* dan *response* sebagai mana di ilustrasikan pada Gambar 2.4 berikut.



Gambar 2. 4 Gambar komunikasi SIP

4. SIP Request

SIP request adalah suatu pesan permintaan dari client kepada server untuk menjalin komunikasi. Pesan-pesan tersebut adalah sebagaimana dijelaskan dalam tabel 2.1 .

Tabel 2. 1 Tabel keterangan SIP *request*.

Pesan Request	Keterangan
INVITE	Mengundang user agent lain untuk bergabung dalam sesi komunikasi

Pesan Request	Keterangan
INVITE	Mengundang user agent lain untuk bergabung dalam sesi komunikasi
ACK	Konfirmasi bahwa user agent telah menerima pesan terakhir dari serangkaian pesan INVITE.
BYE	Terminasi sesi
CANCEL	Membatalkan INVITE
REGISTER	Registrasi di register server
OPTIONS	Meminta informasi tentang kemampuan server
INFO	Digunakan untuk membawa pesan informasi lainnya seperti informasi inline DTMF

5. SIP Response

SIP response merupakan tanggapan dari server terhadap permintaan client. Setiap pesan yang ditampilkan akan dijelaskan pada tabel 2.2 .

Tabel 2. 2 Tabel keterangan SIP *response*.

Pesan Request	Keterangan
1xx	Pesan yang memberikan informasi Contoh : 180 Ringing

2xx	Tanggapan Sukses Contoh : 200 OK
3xx	Tanggapan Redirection Contoh : 302 dipindah alih sementara
4xx	Permintaan tidak ditanggapi Contoh : 403 tidak dapat mengakses
5xx	Server tidak dapat melakukan tanggapan Contoh : 504 gateway time-out
6xx	Tidak dapat menghubungi siapapun Contoh : 602 sibuk

2.2 PBX (Internet Protocol Private Branch Exchange)

IP PBX adalah perangkat *switching* komunikasi telepon dan data berbasis teknologi Internet Protocol (IP) yang mengendalikan ekstensi telepon analog (TDM) maupun ekstensi *IP phone*. Fungsi-fungsi yang dapat dilakukan oleh IP PBX antara lain penyambungan, pengendalian, dan pemutusan hubungan telepon; translasi protokol komunikasi; translasi media komunikasi atau transcoding; serta pengendalian perangkat-perangkat IP Teleponi seperti VoIP Gateway, Access Gateway, dan Trunk Gateway.

IP PBX mempunyai kemampuan multilayanan di jaringan IP ke dunia komunikasi teleponi, sehingga memungkinkan semakin banyak layanan komunikasi yang dapat berjalan di atas jaringan IP. Multilayanan tersebut adalah *voicemail*, *voice conference*, *Interactive Voice Response (IVR)*, *Automatic Call Distribution (ACD)*, *Computer Telephony Integration (CTI)*, *Unified Messaging System (UMS)*, *fax server*, *fax on demand*, *Call Recording System*, *Billing System*, serta *Web-based Management System*.

Asterisk adalah sebuah perangkat lunak telepon IP PBX yang dibuat tahun 1999 oleh Mark Spencer dari Digium. Seperti halnya PBX, asterisk

memungkinkan telepon dapat membuat panggilan ke telepon lain baik antar *IP-phone* atau ke layanan telepon PSTN.

IP PBX memiliki beberapa komponen pendukung komunikasi . Komponen tersebut adalah Data Account Extension, Data Account Trunk, dan Dial Plan.

1. Data Account Extension

Data account extension adalah data account yang akan digunakan oleh extension agar terhubung dengan IP PBX. Extension disini adalah sebuah nama atau nomor yang merepresentasikan user dari IP PBX tersebut.

2. Data Account Trunk

Data account trunk adalah data account yang akan digunakan IP PBX untuk menghubungi trunk. Trunk adalah sebuah nama atau nomor yang merepresentasikan server lain atau IP PBX lain yang akan dihubungi oleh IP PBX ini.

3. Dial Plan

Dial Plan merupakan aturan dial yang akan dimanfaatkan oleh extension untuk menghubungi sesama extension atau trunk sebaliknya.

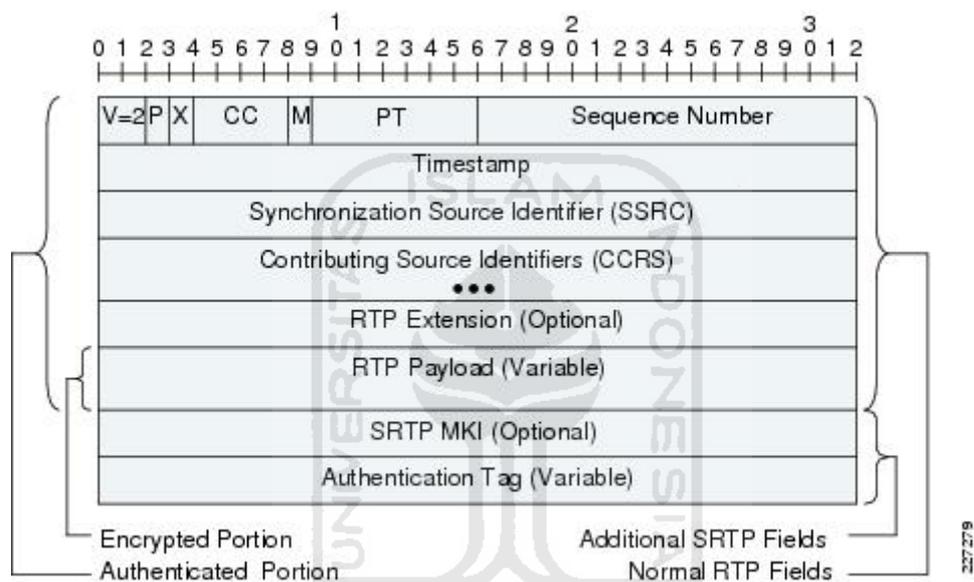
2.3 SRTP (Secure Real Time Protocol)

Pada dasarnya paket data suara yang lewat dalam jaringan komunikasi VoIP tidak dienkripsi. Hal ini memungkinkan adanya penyadapan atau *sniffing* dan membuat rentan keamanan komunikasi tersebut.

Secure real-time protocol adalah salah satu solusi mengatasi masalah tersebut. SRTP digunakan untuk menjaga kerahasiaan data dan autentikasi pesan, serta menjaga lalu lintas paket data RTP atau RTCP.

2.3.1 Susunan SRTP

SRTP adalah tambahan pada paket RTP yang disajikan dalam aliran yang berbentuk tumpukan dimana aplikasinya terletak diantara aplikasi RTP dan layer transport. Aliran paket data yang dikirim oleh RTP akan disaring oleh SRTP dan kemudian dialirkan kembali dengan paket data yang mirip dengan aslinya tetapi sudah dilindungi oleh SRTP pada saat diterima oleh penerima.



Gambar 2. 5 Gambar skema SRTP header.

Pada Gambar 2.5 diatas terdapat *encrypted portion* yaitu bagian RTP yang disaring dan dienkripsi oleh SRTP, kemudian disajikan dalam bentuk yang mirip dengan paket RTP. Perubahan ini menghasilkan penambahan bagian baru pada SRTP yang mengakibatkan ukuran paket menjadi lebih besar.

MKI (Master Key Identifier) dapat dikonfigurasi secara optional. Key management mendefinisikan, memberi tanda dan menggunakan MKI untuk penguncian kembali dan identifikasi bagian master key dengan menggunakan konteks kriptografi. *Authentication tag* dibutuhkan untuk mengkonfigurasi

panjang data. Bagian ini memastikan data tersebut sebagai pesan. Bagian autentikasi dalam paket SRTP berisi RTP header yang diikuti oleh bagian yang terenkripsi dalam paket SRTP.

Pada sisi pengirim, paket data akan di enkripsi terlebih dahulu sebelum di autentikasi. Sedangkan pada sisi penerima data akan di dekripsi dahulu baru di autentikasi.

2.3.2 LibSRTP

LibSRTP merupakan perangkat lunak *open source*. Library ini digunakan untuk implementasi SRTP yang dikembangkan oleh Cisco. Pustaka ini mendukung beberapa fitur yang ada pada SRTP. Fitur yang didukung oleh libSRTP adalah:

1. *Master Key Identifier*

MKI digunakan dengan tujuan penguncian kembali, identifikasi bagian master key dengan menggunakan konteks kriptografi.

2. *Key Derivation*

Key derivation digunakan untuk menentukan kunci-kunci dalam setiap sesinya.

2.4 QoS (Quality of Service)

Dalam dunia jaringan komputer dan jaringan komunikasi terdapat mekanisme penjagaan kualitas layanan. QoS (*Quality of service*) adalah kemampuan untuk membedakan prioritas antara aplikasi, pengguna dan arus data, atau untuk menjamin perbedaan kinerja dari arus data. Sebagai contoh, QoS memungkinkan penjaminan *bitrate*, *delay*, *jitter*, *paket dropping* dan atau kesalahan *bitrate*. penjaminan QoS merupakan hal yang penting dalam jaringan dengan kapasitas yang terbatas, khususnya untuk aplikasi multimedia *streaming realtime* seperti VoIP, game Online dan IP-TV, selama masih membutuhkan ketepatan *bitrate* dan *delay* yang sensitif, dan dalam keterbatasan sumberdaya jaringan.

Dalam bidang telepon, QoS ditetapkan dalam standar ITU X.902 sebagai “*A set of quality requirements on the collective behavior of one or more objects*” [WKI11]. QoS meliputi layanan pada semua aspek konektivitas, seperti pelayanan waktu respon (*respon time*), *loss*, rasio *signal-to-noise*, *cross-talk*, *echo*, *interrupts*, respon frekuensi tingkat kenyaringan suara dan lain-lain. Bagian lain dari QoS telepon adalah GOS (*Grade of Service*), yaitu aspek kapasitas koneksi dan jangkauan jaringan, misalnya penjaminan kemungkinan pemblokiran koneksi dan kemungkinan penghentian kinerja.

Untuk pencarian nilai hasil QoS diperlukan perangkat lunak pendukung untuk memantau arus data saat koneksi dijalankan dan memunculkan nilai-nilai yang dianggap penting.



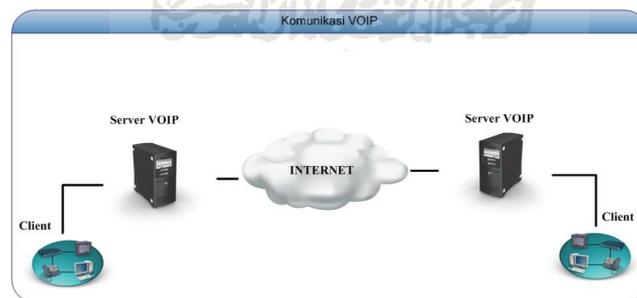
BAB III

METODOLOGI

3.1 Analisis Masalah

VoIP menggunakan protokol UDP. *User* atau *Caller* melakukan *dial* ke ekstensi tertentu yang sudah terdaftar dalam server VoIP melalui protokol *signalling* SIP dan data suara dibawa dengan menggunakan protokol RTP. Protokol ini rawan penyadapan karena data suara yang di bawa tidak di amankan, oleh karena itu di gunakan teknologi SRTP untuk mengamankan paket data tersebut. SRTP mengamankan dengan melakukan enkripsi pengiriman data terlebih dahulu sebelum dikirimkan.

Dengan menggunakan SRTP, terjadi perubahan bentuk paket yang dikirmkan. Jika melihat konsep perbandingan terbalik antara keamanan dengan kualitas, maka munculah permasalahan sejauh mana dampak penggunaan SRTP ini terhadap kualitas layanan. Gambaran umum implementasi VoIP dapat di lihat pada gambar 3.1 berikut



Gambar 3. 1 Gambaran umum implementasi VoIP

Dengan adanya perubahan ukuran paket tersebut maka dimungkinkan akan terjadi perubahan nilai pada delay, jitter dan paket loss. Karena

3.2 Implementasi sistem

Dalam implementasi sistem memiliki dua bagian utama, yaitu kebutuhan perangkat lunak dan kebutuhan perangkat keras.

3.2.1 Kebutuhan Perangkat Lunak

Berikut adalah perangkat lunak yang digunakan:

1. Ubuntu 10.10 Server Edition

Pada penelitian ini digunakan Ubuntu Server 10.10 untuk menjalankan Asterisk SRTP. Sistem ini berfungsi sebagai server VoIP. Pertimbangan menggunakan sistem ini karena lebih mudah dalam implementasi Asterisk dengan SRTP.

2. LibSRTP

LibSRTP adalah *library* perangkat lunak *open source* dalam implementasi SRTP. LibSRTP dikembangkan oleh Cisco System. LibSRTP digunakan karena telah mendukung sistem enkripsi data dengan algoritma enkripsi AES128.

3. IPPBX Asterisk untuk VoIP SRTP

Asterisk adalah perangkat lunak PBX yang di kembangkan oleh Mark Spencer dalam bentuk perangkat lunak bebas, dan hanya dapat di jalankan pada sistem operasi Linux

4. Wireshark

Wireshark adalah perangkat lunak analisis paket jaringan (*network packet analyzer*) open source yang berfungsi untuk menangkap aliran paket data dan menampilkannya dengan rinci dan detail. Kelebihan lain adalah tampilan yang *user friendly* dan sangat fungsional. Dalam dunia keamanan komputer perangkat lunak ini sering digunakan untuk pencurian paket data atau sniffing. Software ini digunakan untuk melakukan identifikasi aliran paket data apakah dengan RTP atau dengan SRTP.

5. Eyebeam 1.5

Eyebeam *softphone* adalah bentuk *user agent* yang digunakan untuk memulai, menerima, dan mengakhiri sesi komunikasi. Alasan pemilihan *softphone* ini karena telah mendukung enkripsi data suara pada real-time protocol sehingga mendukung dalam penggunaan SRTP pada Asterisk.

6. VQ.Manager

VQManager adalah salah satu perangkat lunak untuk melakukan penilaian kualitas terhadap paket data suara. Software ini dipilih karena user-friendly dengan tampilan web yang simple dan lengkap beserta grafik dalam menampilkan perhitungan kualitas layanan suara.

3.2.2 Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan meliputi 1 unit komputer sebagai server dan 2 unit komputer sebagai klien.

1. Kebutuhan Server

Server pada implementasi ini menggunakan komputer dengan spesifikasi minimal berikut :

1. processor IV 2,4 GHz
2. Harddisk 5 Gb, sebagai minimal untuk instalasi sistem ubuntu server 10.10
3. Ethernet card
4. Memory 512 MB
5. CD-ROM

2. Kebutuhan Klien

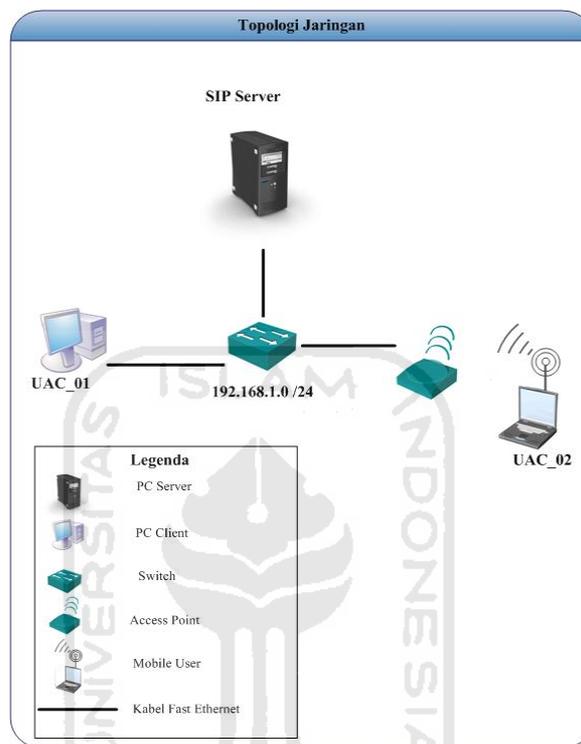
Kebutuhan hardware klien meliputi 2 unit komputer dengan spesifikasi minimal sebagai berikut:

1. Pentium IV 2,4 GHz
2. Memory 512 MB
3. Harddisk 40 GB

4. Ethernet card

3.3 Topologi

Gambar 3.2 menunjukkan topologi yang digunakan pada implementasi .



Gambar 3. 2 Gambar topologi jaringan

3.4 Konfigurasi

3.4.1 Konfigurasi server

Pada implementasi ini penulis berasumsi bahwa installasi Ubuntu 10.10 server edition, LibSRTP, dan Asterisk SVN sudah dilakukan lebih awal.

Pada server Asterisk-SRTP terdapat minimal 3 bagian yang perlu dikonfigurasi, yaitu pada interface.conf untuk pengalamatan IP address, sip.conf dan extension.conf. Pertama kali yang perlu dilakukan adalah pengalamatan IP .

Konfigurasi di lakukan pada file */etc/network/interface.conf* dapat dilihat pada Tabel 3.1 sebagai berikut

Tabel 3. 1 Konfigurasi alamat IP

```
auto eth0
iface eth0 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
```

Tabel 3. 2 Konfigurasi pada sip.conf

```
[authentication]
[123]
type=friend
username=123
secret=123
host=dynamic
context=main
nat=no
srtpcapable=yes

[124]
type=friend
username=124
secret=124
host=dynamic
context=main
nat=no
srtpcapable=yes
```

Pada tabel 3.2 menjelaskan pemberian SIP user, pemberian izin menggunakan SRTP di lakukan pada `srtpcapable=yes`.

Selanjutnya pada file `extensions.conf` dilakukan konfigurasi untuk pemberian *dialplan*. *Dialplan* adalah algoritma yang mengontrol ekstensi panggilan apabila ada panggilan keluar dan panggilan masuk pada IPPBX. Pada Tabel 3.3 adalah konfigurasi *dialplan* yang perlu dilakukan agar dapat menjalankan jika ada permintaan telpon dengan ataupun tanpa menggunakan enkripsi.

Tabel 3. 3 Konfigurasi `extensions.conf`.

```

exten => 123,1,NoOp(Everyone that supports encryption will
have it!)
exten => 123,n,Set _SIPSRTP=${SIPPEER(${EXTEN},srtpcapable)}
exten => 123,n,Dial(SIP/${EXTEN})
exten => 123,n,Hangup

exten => 124,1,NoOp(Everyone that supports encryption will
have it!)
exten => 124,n,Set(_SIPSRTP=${SIPPEER(${EXTEN},srtpcapable)})
exten => 124,n,Dial(SIP/${EXTEN})
exten => 124,n,Hangup

```

Pada konfigurasi ekstensi *dialplan* terdapat 3 bagian, `exten =>` ekstensi, prioritas, perintah (parameter).

Pada baris kedua menunjukkan perintah bahwa jika terdapat SIP user masuk atau keluar dengan ekstensi 123 menggunakan ataupun tanpa enkripsi maka akan diteruskan. Jika tanpa menerapkan algoritma sejenis maka semua panggilan yang menggunakan enkripsi akan di hentikan.[AST11]

3.4.2 Konfigurasi klien

Konfigurasi klien dilakukan pada setiap SIP user. Pada klien software yang digunakan adalah sebagai berikut:

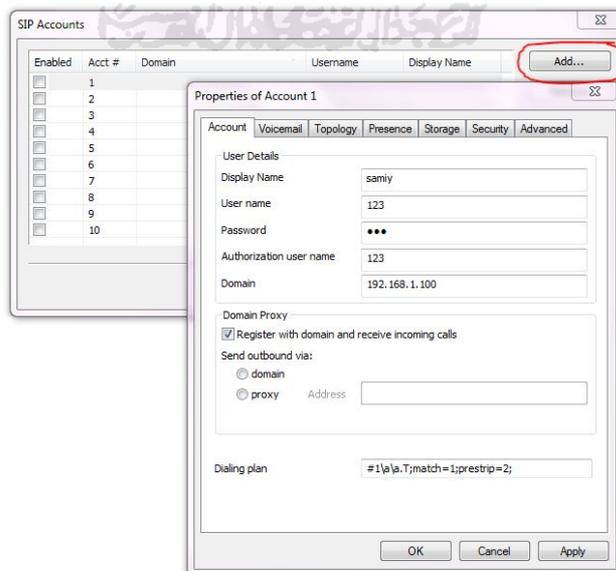
1. Konfigurasi Eyebeam 1.5 *Softphone*

Eyebeam adalah salah satu aplikasi *softphone*. Konfigurasi yang perlu dilakukan adalah pemberian SIP Account dan nomor telepon seperti ditunjukkan pada gambar 3.3



Gambar 3. 3 Pendaftaran SIP Account

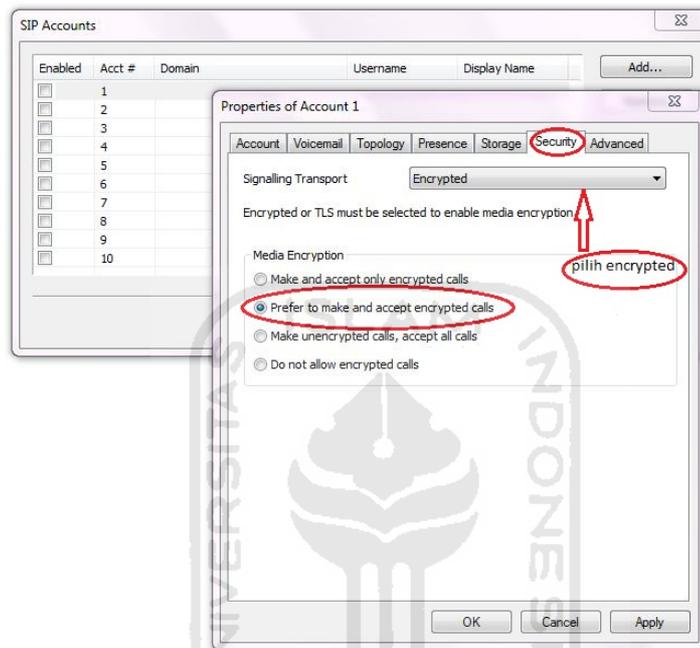
Selanjutnya akan muncul window untuk mendaftarkan *user* seperti pada gambar 3.4.



Gambar 3. 4 Pemberian SIP Account

Pada *field* user name dan password diisikan sesuai SIP *user* yang telah di daftarkan pada sip.conf

Selanjutnya adalah konfigurasi supaya klien dapat melakukan telpon dengan enkripsi seperti ditunjukkan seperti pada gambar 3.5



Gambar 3.5 Pemilihan metode penggunaan enkripsi

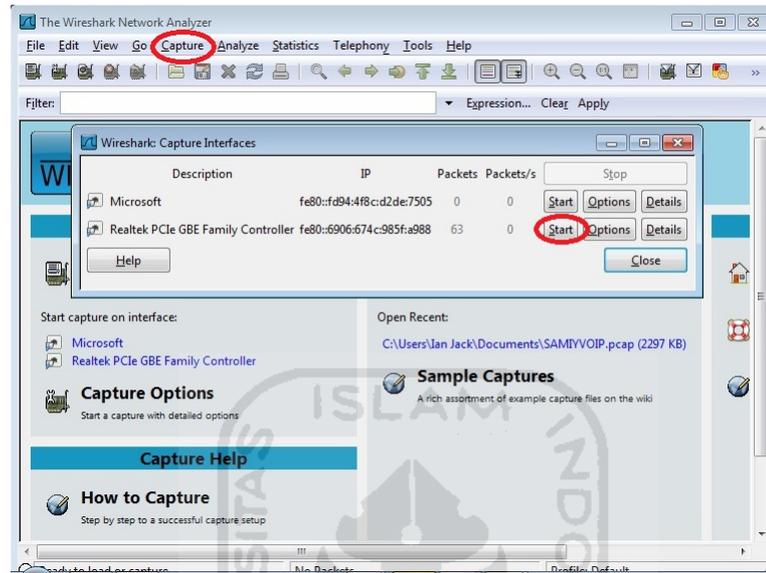
Gambar 3.5 menunjukkan bahwa *encrypted* harus dipilih pada signalling protocol agar komunikasi yang digunakan dapat di enkripsi. Apabila akan melakukan telpon tanpa menggunakan enkripsi pilih *Automatic* pada bagian *Signalling transport*.

2. Konfigurasi wireshark

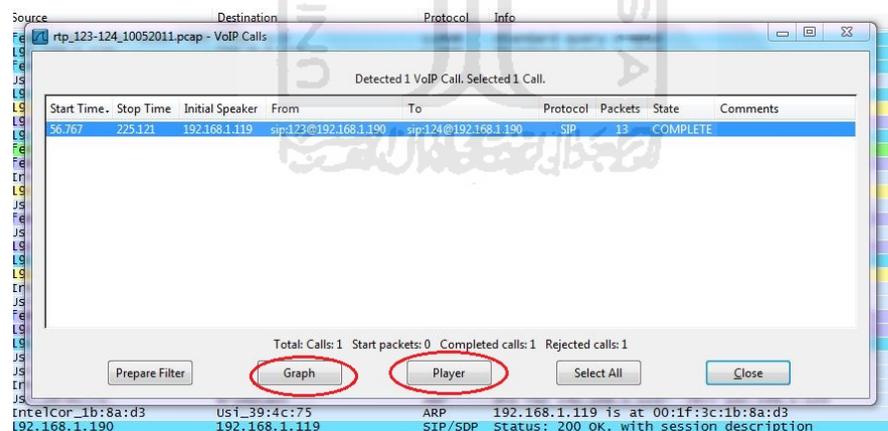
Konfigurasi yang perlu dilakukan pada wireshark antara lain memilih *interface* yang akan digunakan dalam koneksi VoIP.

Gambar 3.6 menunjukkan pemilihan *interface* yang dilalui paket data pada wireshark. Selanjutnya wireshark akan membaca setiap paket yang lewat pada *interface* yang di pilih. Ketika ada panggilan VoIP, wireshark akan membaca

paket protokol SIP dan paket media data baik RTP atau SRTP. Gambar 3.7 menunjukkan menu *toolbar telephony* pilih *VoIP Calls* untuk melihat data VoIP, melihat grafik signalling SIP, dan memutar ulang hasil rekaman perbincangan.

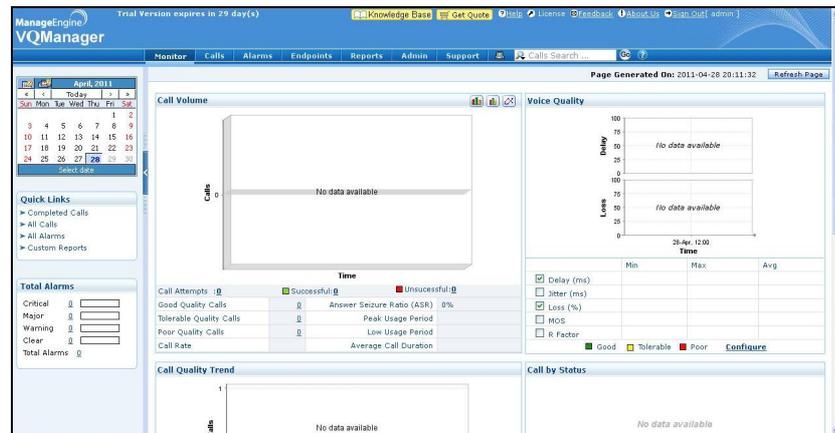


Gambar 3. 6 Gambar pemilihan *interface*



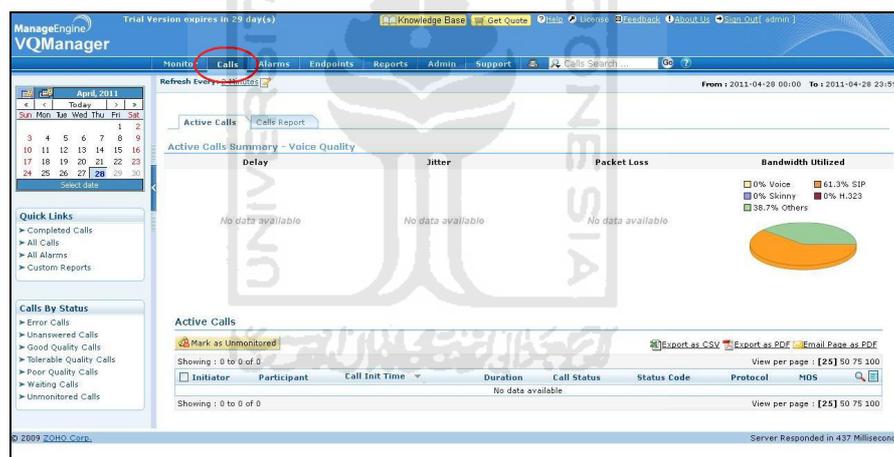
Gambar 3. 7 Gambar VoIP Calls

Jika menggunakan protokol RTP maka hasil rekaman dapat didengar tetapi jika menggunakan protokol SRTP hasil rekaman akan nampak kacau dan tidak dapat didengar. Tampilan dapat dilihat pada gambar 3.8



Gambar 3. 9 Gambar halaman VQManager

Gambar 3.10 memperlihatkan *delay*, *jitter*, *packet loss* dari *service* yang sedang di jalankan dalam bentuk barometer.



Gambar 3. 10 Gambar *monitoring Delay, Jitter dan Packet Loss*

3.5 Rencana Pengujian

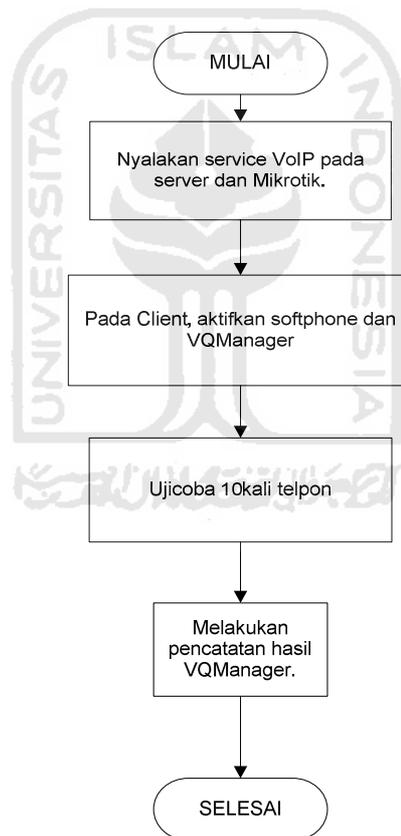
Skenario pada penelitian ini adalah dengan melakukan pengujian telepon antar klien menggunakan protokol RTP dan SRTP dan melihat perbedaan yang didapat dengan parameter delay, jitter dan paket loss pada kapasitas bandwidth yang berbeda-beda.

Pengujian data yang akan dilakukan adalah dengan melakukan uji coba panggilan telepon selama 30 detik antar klien. Pengujian ini dilakukan sebanyak

10 kali percobaan baik menggunakan protokol RTP dan 10 kali menggunakan protokol SRTP.

Pengambilan data dilakukan menggunakan software VQManager untuk melihat delay, jitter, dan paket loss. Sedangkan untuk pembagian bandwidth menggunakan Mikrotik. Setelah didapatkan hasil dari VQManager maka akan dilakukan perbandingan data baik menggunakan protokol RTP dan protokol SRTP untuk masing-masing besaran bandwidth. Besaran bandwidth yang digunakan adalah 64kb, 128kb, 512kb, dan 1Mb.

Berikut flowchart pengujian yang dilakukan.



Gambar 3. 11 Flowchart pengujian.

BAB IV

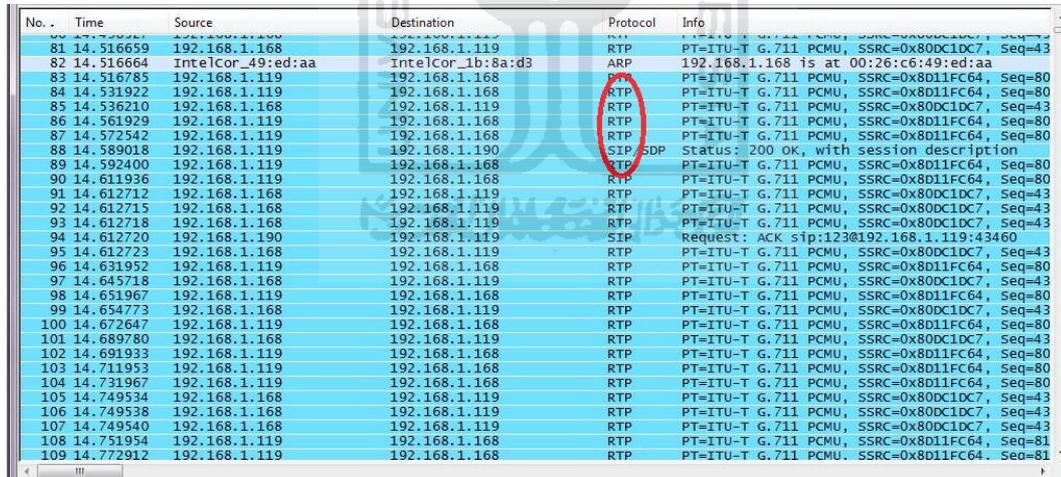
HASIL DAN PEMBAHASAN

4.1 Hasil dan Pembahasan Protokol RTP dan SRTP

Pengujian pada protokol RTP dan SRTP menitikberatkan pada nilai QoS masing-masing protokol, dilihat dari segi keamanan dan performa protokol RTP dan SRTP pada jaringan lokal dengan variasi bandwidth yaitu 64kb, 128kb, 256kb, dan 1Mb.

Pengujian ini dilakukan dengan menggunakan wireshark untuk melihat protokol yang sedang berjalan. Terdapat perbedaan saat menggunakan RTP dan SRTP. Gambar 4.1 menampilkan wireshark saat menangkap paket

RTP.



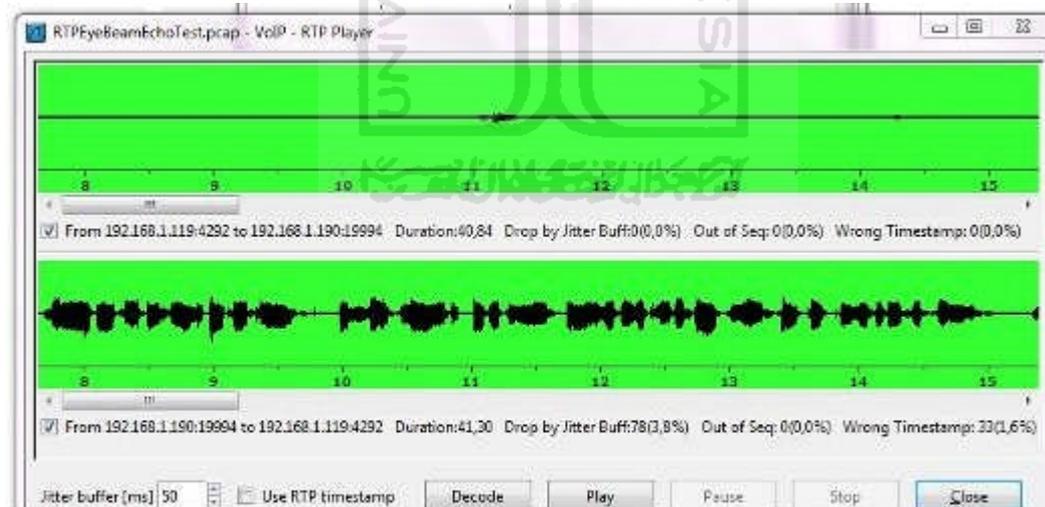
No.	Time	Source	Destination	Protocol	Info
81	14.516659	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
82	14.516664	IntelCor_49:ed:aa	IntelCor_1b:8a:d3	ARP	192.168.1.168 is at 00:26:c6:49:ed:aa
83	14.516785	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
84	14.531922	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
85	14.536210	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
86	14.561929	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
87	14.572542	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
88	14.589018	192.168.1.119	192.168.1.190	SIP	SDP Status: 200 OK, with session description
89	14.592400	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
90	14.611936	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
91	14.612712	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
92	14.612715	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
93	14.612718	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
94	14.612720	192.168.1.190	192.168.1.119	SIP	Request: ACK sip:123@192.168.1.119:43460
95	14.612723	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
96	14.631952	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
97	14.645718	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
98	14.651967	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
99	14.654773	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
100	14.672647	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
101	14.689760	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
102	14.691933	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
103	14.711953	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
104	14.731967	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=80
105	14.749534	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
106	14.749538	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
107	14.749540	192.168.1.168	192.168.1.119	RTP	PT=ITU-T G.711 PCMU, SSRC=0x80DC1DC7, Seq=43
108	14.751954	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=81
109	14.772912	192.168.1.119	192.168.1.168	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8D11FC64, Seq=81

Gambar 4. 1 Tampilan wireshark capture paket RTP.

No.	Time	Source	Destination	Protocol	Info
117	15.939491	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
118	15.949675	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
119	15.965116	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
120	15.968983	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
121	15.987210	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
122	15.988988	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
123	15.999964	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
124	16.008968	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
125	16.021442	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
126	16.029097	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
127	16.042344	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
128	16.049127	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
129	16.059481	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
130	16.068973	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
131	16.082260	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
132	16.089031	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
133	16.100225	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
134	16.109004	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
135	16.120068	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
136	16.129009	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
137	16.139444	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
138	16.149069	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
139	16.167566	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
140	16.168971	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
141	16.184917	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
142	16.188984	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
143	16.209017	192.168.1.119	192.168.1.190	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x2D08EE39, Seq=20
144	16.209564	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64
145	16.219824	192.168.1.190	192.168.1.119	SRTP	PT=ITU-T G.711 PCMU, SSRC=0x758971c4, Seq=64

Gambar 4. 2 Tampilan hasil capture paket data SRTP

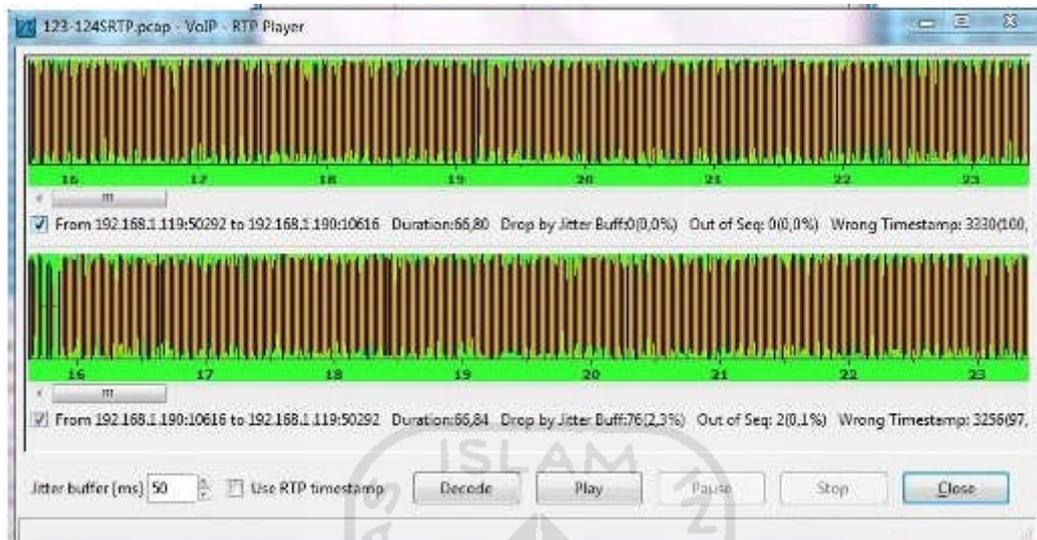
Selain itu wireshark juga dapat merekam dan memutar ulang hasil komunikasi tersebut. Dengan menggunakan protokol RTP, hasil rekaman komunikasi VoIP dapat didengar dengan jelas. Pada Gambar 4.2 menampilkan wireshark saat melakukan putar ulang hasil rekaman komunikasi VoIP.



Gambar 4. 3 Tampilan putar ulang rekaman paket RTP

Namun hasil akan berbeda jika menggunakan SRTP, dengan menggunakan protokol SRTP, sniffer dapat merekam dan memutar ulang hasil

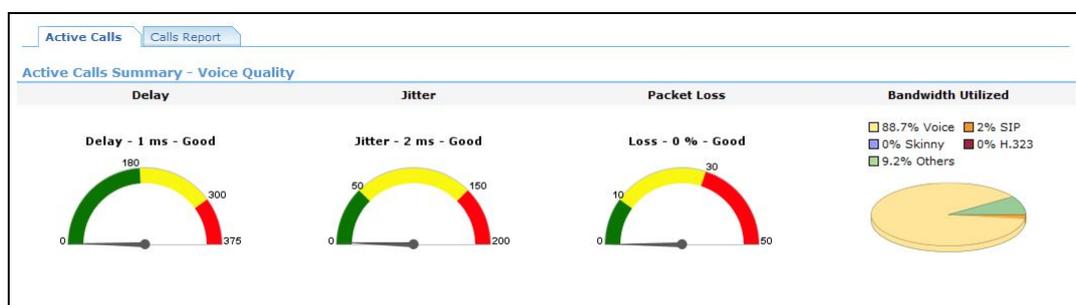
rekaman tetapi tidak dapat terdengar percakapan tersebut karena paket data telah di enkripsi seperti terlihat pada Gambar 4.4.



Gambar 4. 4 Tampilan putar ulang hasil rekaman SRTP.

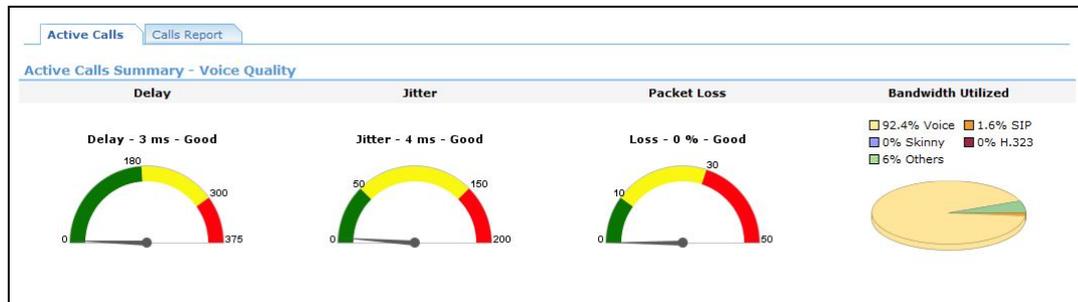
4.2 Perbandingan Hasil Pengamatan

Pengamatan dilakukan menggunakan software VQManager untuk melihat parameter delay, jitter, dan packet loss dalam bentuk barometer. Dalam gambar 4.7 dapat terlihat nilai delay sebesar 1 ms, jitter sebesar 2 ms dan packet loss sebesar 0% dari pengujian penguuan protokol RTP yang telah dilakukan.



Gambar 4. 5 Tampilan barometer pengukuran paket RTP.

Sedangkan pengamatan saat penggunaan protokol SRTP dapat dilihat pada Gambar 4.8. Terlihat pada gambar nilai delay sebesar 3 ms, jitter sebesar 4 ms, dan packet loss sebesar 0%.



Gambar 4. 6 Tampilan barometer pengukuran paket SRTP

Untuk mendapatkan hasil yang lebih pasti maka pengujian dilakukan sebanyak 10 kali pada tiap-tiap ukuran bandwidth yang digunakan. Hal ini dimaksudkan untuk mengetahui bandwidth minimal yang dapat digunakan namun tetap dalam menjaga kualitas dan keamanan. Dari 10 kali pengujian yang dilakukan mendapatkan beberapa variasi hasil, pada tabel dibawah ini menunjukkan hasil kualitas yang didapat pada tiap-tiap ukuran bandwidth yang digunakan.

Dalam komunikasi VoIP kapasitas bandwidth juga diperhitungkan, besarnya kapasitas bandwidth juga mempengaruhi kualitas suara yang didengar oleh user. Pada tabel berikut adalah perbandingan kualitas pada RTP dan SRTP terhadap beberapa lebar bandwidth.

Berikut pada tabel 4.2 menampilkan pengujian pada penggunaan bandwidth 64kb, 128kb, 512kb, 1Mb.

Tabel 4. 1 hasil rata-rata perhitungan RTP dan SRTP dengan bandwitdh 64kb.

Hasil Data Uji Performa RTP dan SRTP dengan 64kb bandwidht						
Pengujian	RTP			SRTP		
	Delay	Jitter	Packet loss	Delay	Jitter	Packet loss
1	1	23	8	6	5	0
2	3	20	10	5	3	0
3	1	5	3	4	4	0
4	2	25	9	6	7	0
5	1	3	2	5	5	0
6	1	14	7	7	4	3
7	2	20	8	4	3	0
8	1	2	10	2	2	1
9	0	3	4	4	3	2
10	1	2	4	5	4	0
rata-rata	1,3	11,7	6,5	4,8	4	0,6

Tabel 4. 2 Hasil rata-rata perhitungan RTP dan SRTP dengan bandwitdh 128kb.

Hasil Data Uji Performa RTP dan SRTP dengan 128kb bandwidht						
Pengujian	RTP			SRTP		
	Delay	Jitter	Packet loss	Delay	Jitter	Packet loss
1	1	14	0	4	4	0
2	2	8	0	3	6	0
3	2	11	0	3	5	0
4	1	5	0	4	5	0
5	0	6	0	5	4	0
6	1	14	0	4	5	0
7	0	7	0	4	3	0
8	2	2	0	2	2	0
9	0	3	0	4	3	0
10	1	2	0	5	4	0
rata-rata	1	7,2	0	3,8	4,1	0

Tabel 4. 3 Hasil rata-rata perhitungan RTP dan SRTP dengan bandwidth 512kb.

Hasil Data Uji Performa RTP dan SRTP dengan 512kb bandwidht						
Pengujian	RTP			SRTP		
	Delay	Jitter	Packet loss	Delay	Jitter	Packet loss
1	0	8	0	3	4	0
2	1	4	0	4	5	0
3	2	6	0	4	4	0
4	1	9	0	3	4	0
5	2	8	0	3	4	0
6	1	6	0	7	4	0
7	0	7	0	4	3	0
8	1	2	0	2	2	0
9	0	3	0	4	3	0
10	1	2	0	5	4	0
rata-rata	0,9	5,5	0	3,9	3,7	0

Tabel 4. 4 Hasil rata-rata perhitungan RTP dan SRTP dengan bandwidth 1Mb.

Hasil Data Uji Performa RTP dan SRTP dengan 1Mb bandwidht						
Pengujian	RTP			SRTP		
	Delay	Jitter	Packet loss	Delay	Jitter	Packet loss
1	2	2	0	4	3	0
2	0	3	0	3	3	0
3	1	4	0	2	3	0
4	1	2	0	1	2	0
5	2	6	0	2	2	0
6	1	2	0	7	4	0
7	0	2	0	4	3	0
8	1	2	0	2	2	0
9	0	3	0	4	3	0
10	1	2	0	5	4	0
rata-rata	0,9	2,8	0	3,4	2,9	0

Berdasarkan tabel diatas maka dapat dibuat tabel dan grafik perbandingan delay, jitter dan paket loss antara RTP dan SRTP. Berikut pada tabel 4.6 perbandingan delay, dan pada tabel 4.6 menampilkan perbandingan jitter sedangkan pada tabel 4.7 menampilkan perbandingan paket loss.

Tabel 4. 5 Perbandingan delay antara RTP dan SRTP dengan variasi bandwitd.

perbandingan delay dengan bandwidth		
	RTP	SRTP
64kb	1,4	4,8
128kb	1	3,8
512kb	0,9	3,9
1Mb	0,9	3,4

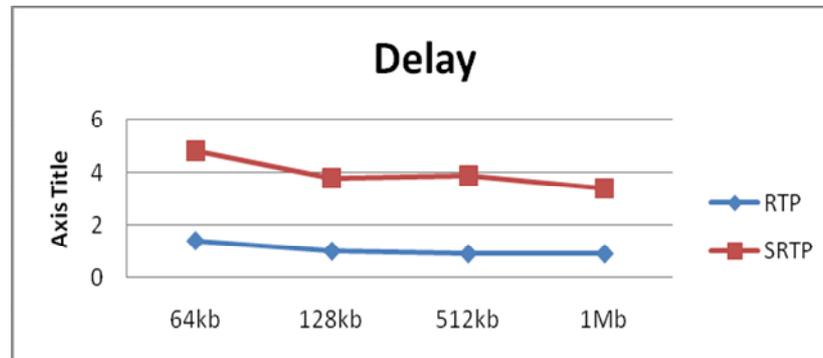
Tabel 4. 6 Perbandingan jitter antara RTP dan SRTP dengan variasi bandwitd.

perbandingan jitter dengan bandwidth		
	RTP	SRTP
64kb	11,7	4
128kb	7,2	4,1
512kb	5,5	3,7
1Mb	2,8	2,9

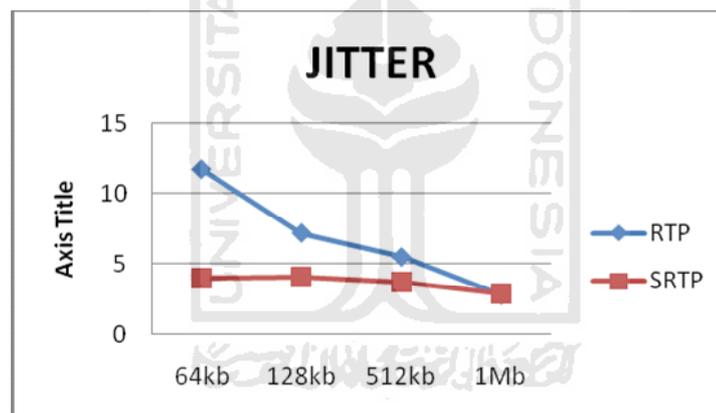
Tabel 4. 7 Perbandingan paket loss antara RTP dan SRTP dengan variasi bandwitd.

perbandingan paket loss dengan bandwidth		
	RTP	SRTP
64kb	6,5	0,6
128kb	0	0
512kb	0	0
1Mb	0	0

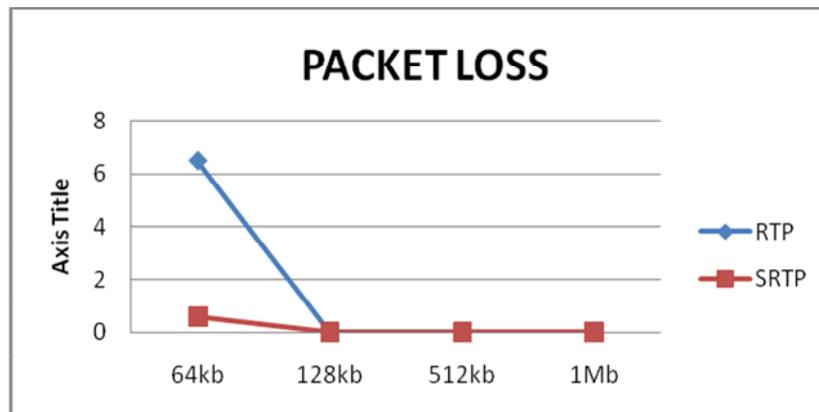
Pada gambar 4.9 berikut adalah grafik dari tabel 4.5. pada grafik tersebut dapat diamati besaran delay yang terjadi saat melakukan panggilan VoIP menggunakan RTP dan SRTP.



Gambar 4. 7 Grafik perbandingan delay saat menggunakan RTP dan SRTP.



Gambar 4. 8 Grafik perbandingan jitter saat menggunakan RTP dan SRTP.



Gambar 4. 9 Gambar grafik perbandingan paketloss saat menggunakan RTP dan SRTP.



BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari hasil penelitian yang dilakukan adalah:

1. SRTP dapat digunakan sebagai salah satu solusi keamanan dalam komunikasi multimedia real-time sebagai pengganti RTP.
2. Dari hasil perbandingan yg dilakukan RTP memiliki nilai QoS lebih baik karena nilai awal yang lebih kecil daripada SRTP dan cenderung lebih baik dengan semakin bertambahnya kapasitas bandwidth yang digunakan. Rincian perbandingan delay, jitter dan paket loss antar RTP dan SRTP sebagaimana dapat dilihat pada grafik gambar 4.7, gambar 4.8 dan gambar 4.9.
3. Berdasarkan faktor bandwidth menunjukkan VoIP akan berjalan dengan stabil jika menggunakan bandwidth di atas 512kb, meskipun dari nilai delay, jitter dan packet loss masih dalam batasan toleransi, namun jika menggunakan bandwidth dibawah 64kb maka paket media tidak dapat berjalan.

5.2 Saran

Dari hasil penelitian yang telah dilakukan terdapat beberapa saran yang perlu disampaikan, antara lain:

1. Agar dapat melakukan penelitian lebih lanjut mengenai karakteristik dan sifat-sifat dari protokol RTP dan SRTP untuk diketahui kelebihan dan kelemahannya.

2. Agar dapat melakukan penelitian lebih lanjut dengan menggunakan TLS (*Transport Layer Security*) untuk mendukung keamanan pada *signalling*.
3. Agar dapat menjadi penelitian lebih lanjut karena data dapat berubah secara fluktuatif dan dapat mencari sebab dari perubahan data tersebut.



DAFTAR PUSTAKA

- [AST11] Anonim, *Asterisk SRTP*, <http://voip-info.org/wiki/page=Asterisk+SRTP>, diakses 20 Februari 2011
- [LIBS11] Anonim, *About libSRTP*, <http://srtp.sourceforge.net/srtp.html> diakses 15 Februari 18 Februari 2011
- [OWP07] Purbo, Onno W, 2007. *VoIP: Cikal Bakal "Telkom Rakyat" (Panduan Lengkap Setting VoIP)*. Infokomputer. Jakarta.
- [RMP11] Philippe, Remi, 2011. *Asterisk SRTP*, <http://www.remiphilippe.fr/2011/01/16/asterisk-srtp-with-1-8/> diakses 2 Maret 2011.
- [TJN10] Joanita, Thania, 2010. Analisis Keamanan Pada Voip Menggunakan Secure Real Time Protocol. UII.
- [WKI11] *Anonim* http://en.wikipedia.org/wiki/Quality_of_service diakses 15 agustus 2011