



**UNIVERSITAS INDONESIA**

**Implementasi dan Analisa Pengaksesan Jaringan dan Kontrol  
QoS Berbasis SIP pada Lingkungan NGN**

**TESIS**

**AGUS AWALUDIN**  
**0906495545**

**FAKULTAS TEKNIK  
PROGRAM STUDI ELEKTRO  
KEKHUSUSAN MULTIMEDIA**

**DEPOK  
JULI 2012**



**UNIVERSITAS INDONESIA**

**Implementasi dan Analisa Pengaksesan Jaringan dan Kontrol QoS berbasis  
SIP pada Lingkungan NGN**

**TESIS**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister  
Teknik**

**AGUS AWALUDIN**  
**0906495545**

**FAKULTAS TEKNIK  
PROGRAM STUDI ELEKTRO  
KEKHUSUSAN MULTIMEDIA**

**DEPOK  
JULI 2012**

## HALAMAN PERNYATAAN ORISINALITAS

Saya menyatakan dengan sesungguhnya bahwa tesis dengan judul :

### **IMPLEMENTASI DAN ANALISA AKSES JARINGAN DAN KONTROL QoS BERBASIS SIP PADA LINGKUNGAN NGN**

yang dibuat untuk melengkapi sebagian persyaratan menjadi Master Teknik pada program studi Teknik Elektro Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia, sejauh yang saya ketahui bukan merupakan tiruan atau duplikasi dari tesis yang sudah dipublikasikan dan atau pernah dipakai untuk mendapatkan gelar kesarjanaan di lingkungan Universitas Indonesia maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Nama : Agus Awaludin

NPM : 0906495545

Tanda Tangan :



Tanggal : 3 Juli 2012

## HALAMAN PENGESAHAN

Tesis ini diajukan oleh :  
Nama : Agus Awaludin  
NPM : 0906495545  
Program Studi : Elektro  
Judul Tesis : Implementasi dan Analisa Akses Jaringan dan Kontrol QoS berbasis SIP Pada Lingkungan NGN

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Teknik pada program studi multimedia, Fakultas Teknik Universitas Indonesia.

Pembimbing : Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng.

Penguji : Prof. Dr. Ir. Bagio Budiarjo, MSc.

Penguji : Yan Maraden, ST. MSc.

Penguji : I Gde Dharma Nugraha, ST. MT.

Ditetapkan di : Depok

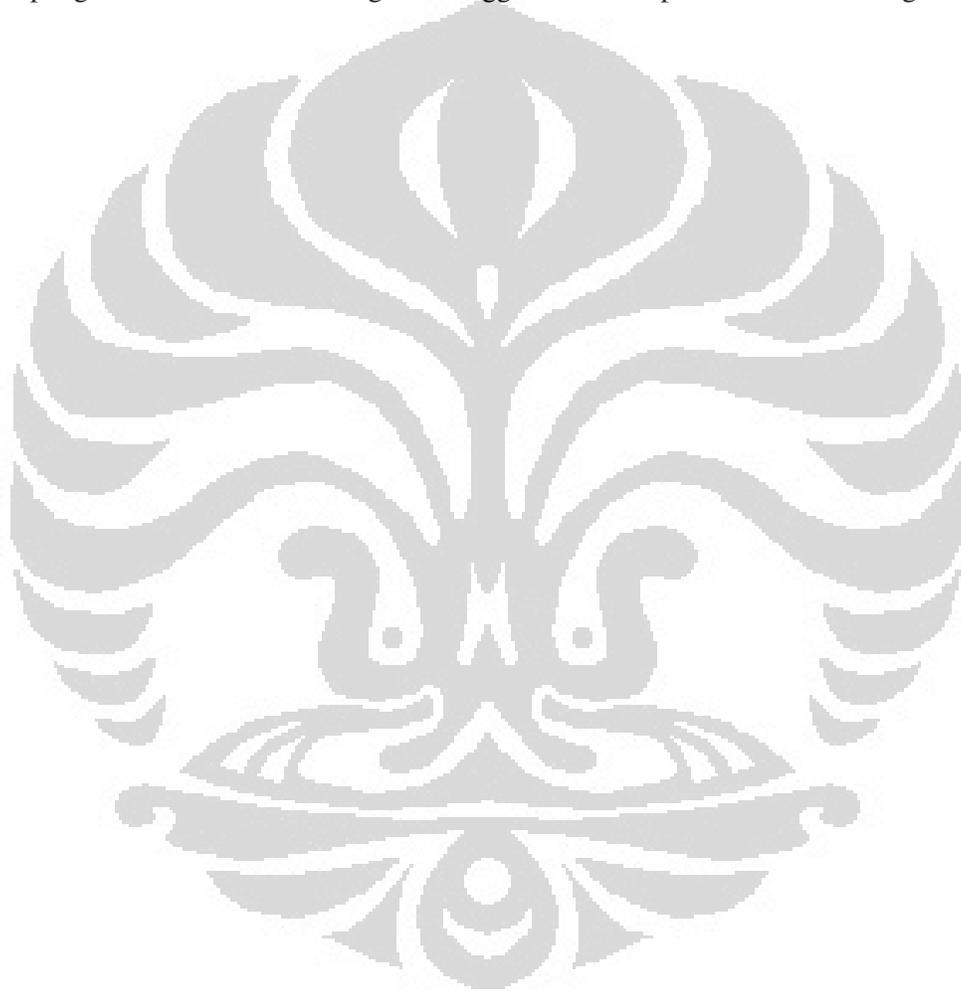
Tanggal : 3 Juli 2012

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada :

Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng.

selaku dosen pembimbing yang telah bersedia meluangkan waktu untuk memberi pengarahan, diskusi, bimbingan sehingga tesis ini dapat diselesaikan dengan baik.



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

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

Nama : Agus Awaludin

NPM : 0906578150

Program Studi : Jaringan Informasi dan Multimedia

Departemen : Teknik Elektro

Fakultas : Teknik

Jenis karya : Tesis

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:

### **IMPLEMENTASI DAN ANALISA AKSES JARINGAN DAN KONTROL QoS BERBASIS SIP PADA LINGKUNGAN NGN**

beserta perangkat yang ada (jika diperlukan). 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 : Depok

Pada tanggal : 3 Juli 2012.



(Agus Awaludin)

## ABSTRAK

Nama : Agus Awaludin  
Program Studi : Teknik Elektro  
Judul : Implementasi dan Analisa Akses Jaringan dan Kontrol QoS berbasis SIP pada Lingkungan NGN  
Pembimbing : Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng.

Infrastruktur layanan telekomunikasi pada *Fixed Network* maupun pada *Mobile Network*, berevolusi dari jaringan berbasis infrastruktur *Switched Circuit Network* (SCN) ke jaringan *Packet Switch Network* (PSN). Pada *Packet Switch Network* interkoneksi dibangun bersifat *Connectionless*, menggunakan kanal komunikasi yang digunakan secara bersama (*Shared*) serta pengelolaan alokasi kanal komunikasi untuk layanan dilakukan dengan menggunakan mekanisme *Statistical Multiplexing*. Layanan telekomunikasi yang bersifat *realtime* kurang baik diadopsi pada *Packet Switch Network*, hal ini adanya kemungkinan *Queuing Delay* dan *Packet Drop* yang disebabkan karakteristik dari *Statistical Multiplexing*. *Statistical Multiplexing* adalah mekanisme paket forwarding yang menggunakan metode *Buffer* dan *Scheduling* dalam meneruskan trafik dari satu network ke network lainnya. Pada tesis ini di rancang dan dikembangkan penerapan manajemen trafik dengan mekanisme berbasis *per-flow* dengan memanfaatkan infrastruktur switch berbasis SIP untuk mengontrol penerapan kebijakan trafik pada jaringan berbasis paket yang dibangun mengacu pada fungsi arsitektur *Policy Based Admission Control* yang didefinisikan oleh IETF. Hasil uji coba menunjukkan keberhasilan penerapan QoS dengan pengkondisian *Throughput* layanan jaringan berdasarkan profil pengguna. Metode tanpa umpan balik antara *Call Session Control Function* (CSCF) dan *Decision Point* (PDP) memiliki kinerja yang mendekati CSCF umumnya, namun pada skenario ini terjadi perbedaan waktu yang cukup berarti antara penyelesaian waktu pemrosesan *SIP Signalling* dan penerapan QoS di sisi *Policy Enforcement Point* (PEP).

Kata kunci: NGN, IMS, IntServ, DiffServ, Campus Network, SIP, LARTC, Policy Based Admission Control

## ABSTRACT

Name : Agus Awaludin  
Study Program : Teknik Elektro  
Title : Implementation and Analysis of Network Access and SIP Based QoS Control in NGN Environment  
Supervisor : Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng.

Next generation of fixed network and Mobile network telecommunication infrastructure and services is evolved from Switched Circuit Network (SCN) based to Packet Switched Network (PSN) based. Within Packet Switched Network interconnection of communication services is built in a connectionless environment, using a shared communication channel and adopt a statistical multiplexing mechanism for forwarding traffic between network. Real time communication services is not smoothly adopted by this type of forwarding mechanism because the queuing delay and packet drop characteristic of statistical multiplexing. This thesis implement per-flow traffic basis management by utilizing SIP based softswitch to control the enforcement of traffic policy on a packet network infrastructure that adopt IETF's Policy Based Admission Control architecture. The successfulness of offered solution is observed in the distribution condition of allocated bandwidth for VoIP traffic compared to other traffic. The experiments show the successful application of throughput conditioning based on SIP user profiles. The performance issue of SIP signalling is addressed by a no feedback scenario between Call Signalling Control Function (CSCF) and Policy Enforcement Point (PEP) but there is a significant difference of completion time on SIP processing and QoS Enforcement

Keywords: NGN, IMS, IntServ, DiffServ, Campus Network, SIP, LARTC, Policy Based Admission Control

## DAFTAR ISI

Halaman Pernyataan Orisinalitas .....	ii
Halaman Pengesahan .....	iii
Ucapan Terimakasih .....	iv
Halaman Pernyataan Persetujuan Publikasi Tugas Akhir untuk Kepentingan Akademis .....	v
Abstrak .....	vi
Abstract .....	vii
Daftar Isi .....	viii
Daftar Gambar .....	x
Daftar Tabel .....	xi
Daftar Singkatan .....	xii
<b>BAB 1. PENDAHULUAN.....</b>	<b>1</b>
1.1. Latar Belakang.....	1
1.2. Tujuan Penulisan .....	2
1.3. Batasan Makalah.....	2
1.4. Sistematika Penulisan .....	2
<b>BAB 2. MANAJEMEN TRAFFIC JARINGAN DAN NGN .....</b>	<b>3</b>
2.1. <i>Multiplexing</i> pada Jaringan Komunikasi.....	3
Gambar 2.1. Diagram <i>Switch</i> .....	3
2.1.1. <i>Multiplexing</i> pada <i>Switched Circuit Network</i> .....	3
2.1.2. <i>Multiplexing</i> pada <i>Packet Switched Network</i> .....	4
2.1.3. Hipotesa Mekanisme <i>Admission Control</i> .....	5
2.2. Manajemen Sumber Daya dan <i>QoS</i> .....	7
2.2.1. <i>Integrated Service</i> .....	7
2.2.2. <i>Differentiated Service</i> .....	8
2.3. Tinjauan Umum NGN.....	9
2.3.1. Arsitektur NGN.....	9
2.3.2. Penerapan <i>QoS</i> pada NGN .....	10
2.3.3. Klasifikasi Protokol NGN.....	12
2.4. Prinsip Protokol Session Initiation Protocol (SIP) .....	13
2.5. Implementasi Manajemen <i>Traffic</i> pada <i>Linux</i> .....	14
2.5.1. Packet Filtering Firewall.....	15
2.5.2 Policy Routing.....	16
2.5.3. <i>Traffic Control</i> .....	17

<b>BAB 3. PERANCANGAN DAN IMPLEMENTASI .....</b>	<b>20</b>
3.1. Skenario Perancangan .....	20
3.2. Arsitektur Rancangan.....	21
3.3. Komponen .....	22
3.3.1. <i>Call Session Control Function</i> (CSCF).....	22
3.3.2. <i>Policy Decission Point</i> (PDP).....	22
3.3.3. <i>Policy Enforcement Point</i> (PEP).....	23
3.4. Penerapan QoS berbasis SIP .....	23
3.4.1. Registrasi SIP UA .....	24
3.4.2. Call Setup dan Teardown.....	25
3.5. Infrastruktur Rancang Bangun .....	26
3.5.1. Lingkungan Kerja Rancang Bangun .....	26
3.5.2. Topologi Pengujian .....	27
<b>BAB 4. PENGUJIAN DAN ANALISA KINERJA .....</b>	<b>28</b>
4.1. Pengaruh Penerapan <i>QoS</i> pada <i>Traffic</i> Jaringan .....	28
4.1.1. Metode Pengujian <i>Throughput</i> .....	30
4.1.2. Hasil Pengujian <i>Throughput</i> .....	30
4.2. Pengaruh pada Pensinyalan.....	32
4.2.1. Metode Pengujian Signalling .....	34
4.1.2. Hasil Pengujian Signalling.....	36
<b>BAB 5. KESIMPULAN .....</b>	<b>37</b>
<b>DAFTAR ACUAN .....</b>	<b>39</b>

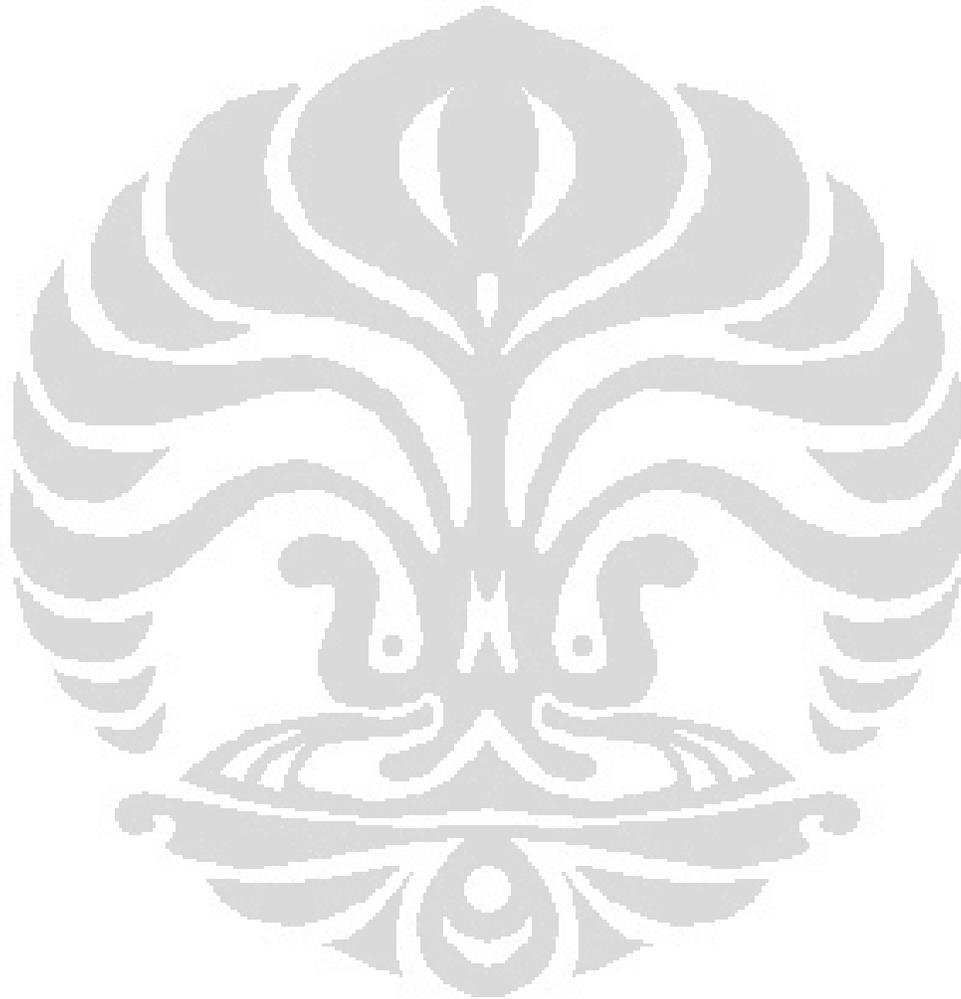
## DAFTAR GAMBAR

Gambar 2.1. Diagram Switch.....	3
Gambar 2.2. <i>Fixed Synchronous Multiplexer</i> .....	4
Gambar 2.3. <i>Statistical Multiplexing</i> .....	5
Gambar 2.4. <i>Hipotesa Admission Control</i> .....	6
Gambar 2.5. <i>Control Plane dan Data Plane pada IntServ</i> .....	7
Gambar 2.6. <i>Admission Control pada IntServ</i> .....	8
Gambar 2.7. <i>Profiling trafik dilakukan oleh Edge Router</i> .....	9
Gambar 2.8. <i>Arsitektur menyeluruh NGN TISPAN</i> .....	10
Gambar 2.9. <i>IETF Architecture of Policy Based Admission Control</i> .....	11
Gambar 2.10. <i>3GPP PCC Architecture</i> .....	11
Gambar 2.11. <i>ETSI TISPAN RACS Architecture</i> .....	12
Gambar 2.12. <i>Protocol NGN</i> .....	13
Gambar 2.13. <i>Komunikasi SIP</i> .....	13
Gambar 2.14. <i>SIP Protokol Call Flow Standar</i> .....	14
Gambar 2.15. <i>Operasi Forwarding Netfilter/IPTABLE</i> .....	15
Gambar 2.16. <i>Operasi NAT Netfilter/IPTABLE</i> .....	16
Gambar 2.17. <i>Classful Queuing Disciplin</i> .....	18
Gambar 3.1. <i>Flowchart kegiatan perancangan</i> .....	20
Gambar 3.2. <i>Pemetaan rancangan terhadap subsistem NGN</i> .....	21
Gambar 3.3. <i>Diagram fungsi pada rancangan arsitektur</i> .....	21
Gambar 3.4. <i>Diagram Penerapan QoS berbasis SIP</i> .....	24
Gambar 3.5. <i>Diagram komunikasi pada registrasi SIP UA</i> .....	24
Gambar 3.6. <i>Diagram komunikasi pada Call Setup and Teardown</i> .....	25
Gambar 3.7. <i>Konfigurasi Lingkungan Pengujian Berbasis Virtualisasi</i> .....	26
Gambar 3.8. <i>Konfigurasi Topologi Pengujian</i> .....	27
Gambar 4.1. <i>Skenario Penerapan QoS</i> .....	28
Gambar 4.2. <i>Metode Pengujian Throughput</i> .....	29
Gambar 4.3. <i>Throughput pada unregistered UE</i> .....	30
Gambar 4.4. <i>% Packet Loss pada unregistered UE</i> .....	31
Gambar 4.5. <i>Jitter pada unregistered UE</i> .....	31
Gambar 4.6. <i>Throughput pada registered UE</i> .....	32
Gambar 4.7. <i>% Packet Loss pada registered UE</i> .....	33
Gambar 4.8. <i>Jitter pada registered UE</i> .....	33
Gambar 4.9. <i>Metode Pengujian Pensinyalan</i> .....	34
Gambar 4.10. <i>Kinerja SIP dengan pemisahan CSCF, PDP dan PEP</i> .....	35
Gambar 4.11. <i>Kinerja SIP dengan CSCF dan PDP pada mesin yang sama</i> .....	35
Gambar 4.12. <i>Kinerja SIP CSCF independen terhadap PDP</i> .....	36

## DAFTAR TABEL

Table 1. Kebijakan default *Policy Routing*

17



## DAFTAR SINGKATAN



IP	<i>Internet Protocol</i>
NGN	<i>Next Generation Network</i>
IMS	<i>IP Multimedia Subsystem</i>
EPC	<i>Evolved Packet Core</i>
QOS	<i>Quality of Service</i>
VOIP	<i>Voice Over IP</i>
SIP	<i>Session Initiation Protocol</i>
UE	<i>User Agent</i>
PCRF	<i>Policy and Charging Rules Function</i>
PCEF	<i>Policy Control Enforcement Function</i>
CBQ	<i>Class Based Queueing</i>
HTB	<i>Hierarchy Token Bucket</i>
RPDB	<i>Routing Policy Database</i>
PRR	<i>Policy Routing Rule</i>
NAT	<i>Network Address Translation</i>
VPN	<i>Virtual Private Network</i>
VLAN	<i>Virtual Local Area Network</i>
WLAN	<i>Wireless Local Area Network</i>
TIK	<i>Teknologi Informasi dan Komunikasi</i>
UA	<i>User Agent</i>
UE	<i>User End Point</i>
IMS	<i>IP Multimedia Subsystem</i>
IETF	<i>Internet Engineering Task Force</i>
AF	<i>Application Function</i>
PDP	<i>Policy Decision Point</i>
PEP	<i>Policy Enforcement Point</i>
ETSI	<i>European Telecommunications Standards Institute</i>
TISPAN	<i>Telecom &amp; Internet converged Service &amp; Protocol for Advance Network</i>
RACS	<i>Resource and Admission Control Subsystem</i>
CSCF	<i>Call Session Control Function</i>

## BAB 1

### PENDAHULUAN

#### 1.1. Latar Belakang

*Roadmap* layanan telekomunikasi telah ditetapkan untuk berpindah dari layanan berbasis infrastruktur *Switched Circuit Network* ke arah penggunaan infrastruktur jaringan *Packet SwitchNetwork* yang berbasiskan teknologi IP. Dalam rangka mengadopsi layanan multimedia dimasa mendatang, dimasa mendatang baik layanan *Fixed Network* dan *Mobile Network* akan berevolusi dari framework *Next Generation Network* (NGN) dan *IP Multimedia Subsystem* (IMS) menjadi *Evolved Packet Core* (EPC) yang merupakan titik temu dari berbagai NGN. Pada *framework* ini protokol berbasis IP seperti SIP memegang peranan penting dalam layanan telekomunikasi. Pada saat ini banyak organisasi dengan jaringan yang besar telah memiliki infrastruktur layanan komunikasi suara dan gambar. Pengelolaan softswitch sebagai pengontrol utama layanan ini telah dapat dikuasai oleh pengelola layanan baik operator telekomunikasi maupun pengelola jaringan organisasi. Hingga saat ini penerapan kebijakan layanan komunikasi multimedia dan pengaksesan layanan jaringan dilakukan secara terpisah dengan infrastruktur dan teknologi yang berbeda. Hal ini berimplikasi proses otorisasi pengaksesan layanan yang bertingkat dan berulang dialami oleh pengguna. Bagi pengelola jaringan, keberadaan infrastruktur yang beragam, dan penerapan kebijakan yang tidak terintegrasi antara layanan komunikasi multimedia dan layanan aplikasi jaringan lainnya menyebabkan sulitnya untuk memberikan kepastian pemenuhan tingkat layanan terkait dengan kebutuhan minimum *bandwith* pengaksesan layanan pengguna.

Penelitian ini bertujuan memanfaatkan fitur teknologi berbasis protokol SIP untuk melakukan fungsi yang lebih kompleks diluar fungsi dasarnya sebagai *Call Control Protocol* untuk melakukan penerapan kebijakan pengaksesan jaringan dan QoS, yang dikombinasikan dengan fitur-fitur teknologi jaringan berbasis Linux, sehingga dapat memberikan garansi QoS dinamis berbasis *per-flow* pada jaringan yang menerapkan model implementasi *DiffServ*.

## 1.2. Tujuan Penulisan

Tujuan dari penelitian ini adalah mengembangkan model jaringan yang dapat menerapkan sistem yang terintegrasi dalam menyediakan pengaksesan layanan dan penerapan QoS dengan memanfaatkan fitur protokol SIP dan manajemen trafik jaringan berbasis Linux.

## 1.3. Batasan Makalah

Permasalahan yang dibahas pada penelitian ini dibatasi pada penyediaan fitur manajemen pengaksesan jaringan berbasis SIP dan penerapan QoS yang dinamis pada Edge Router pada layanan VoIP berbasis SIP.

## 1.4. Sistematika Penulisan

Pembahasan yang dilakukan pada penelitian ini meliputi empat bab, yaitu:

Bab 1 Pendahuluan. Bagian ini terdiri dari latar belakang masalah, tujuan penelitian, batasan masalah dan sistematika penulisan.

Bab 2 Manajemen *Traffic* Jaringan dan NGN. Bagian ini berisi tinjauan Multiplexing pada Switched Circuit Network, dan Packet Switched Network, NGN, prinsip protokol SIP dan penerapan manajemen trafik pada Linux

Bab 3 Perancangan dan Implementasi. Pada Bab ini berisi penjelasan rancangan arsitektur yang meliputi fungsi dan komponen yang dibangun dan keterkaitannya dengan arsitektur *Policy Based Admission Control* dari IETF, rancangan topologi jaringan pengujian

Bab 4 Pengujian dan Analisa Kinerja. Bagian ini berisikan uraian metode pengujian dan analisa hasil pengukuran penerapan QoS dan kinerja *Call Control*.

Bab 5 Kesimpulan. Bagian ini berisikan kesimpulan dan saran pengembangan lebih lanjut.

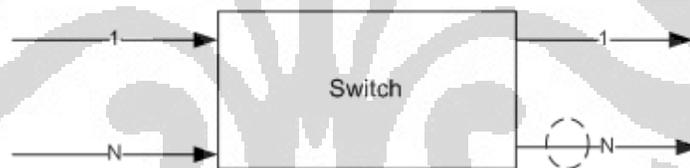
## BAB 2

### MANAJEMEN *TRAFFIC* JARINGAN DAN NGN

#### 2.1. *Multiplexing* pada Jaringan Komunikasi

Infrastruktur jaringan layanan telekomunikasi menghubungkan pengguna layanan melalui fasilitas layanan suara, gambar dan data. Pada infrastruktur ini perangkat *Switch* digunakan untuk menghubungkan satu atau lebih jalur pelanggan ke jaringan layanan komunikasi. Perangkat *Switch* yang ditunjukkan pada Gambar 2.1, memiliki satu atau lebih jalur masukan dan satu atau lebih keluaran yang menghubungkan jalur pelanggan ke jaringan atau menghubungkan dari satu jaringan ke jaringan lainnya.

*Multiplexing* adalah mekanisme yang diterapkan jika terdapat satu atau lebih jalur masukan yang harus diteruskan ke salah satu jalur keluaran. Umumnya penggunaan jalur keluaran digunakan bersama untuk beberapa aliran *traffic* dengan membagi ruang waktu (slot) dalam satu *frame* yang sama.

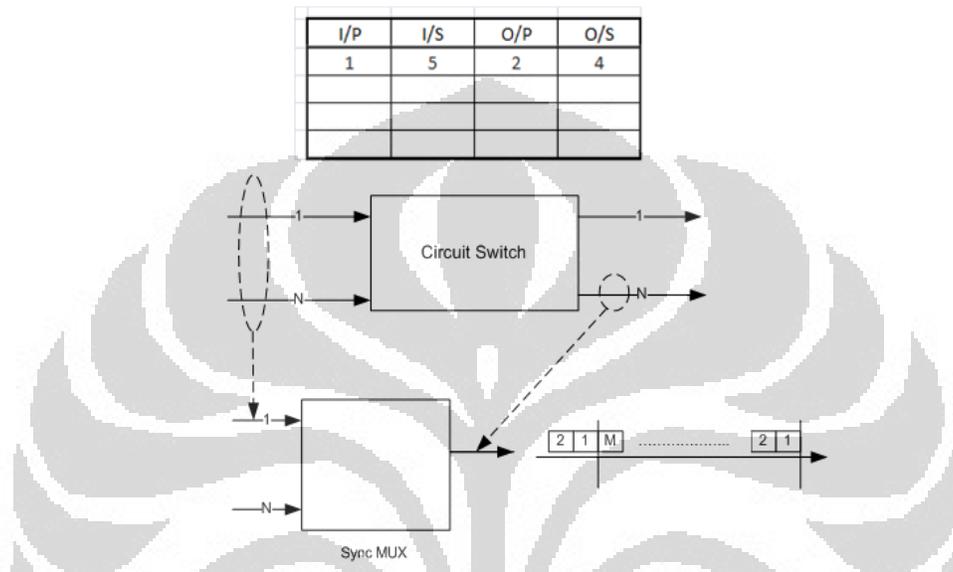


Gambar 2.1. Diagram *Switch* [22]

##### 2.1.1. *Multiplexing* pada *Switched Circuit Network*

Salah satu metode *multiplexing* pada jaringan SCN adalah *Fixed Time Division Multiplexing* (*Fixed TDM*). Pada *fixed TDM*, aliran per *traffic* menduduki urutan slot yang tetap pada *frame*. Sebagai contoh pada satu waktu ada masukan dari kanal input 1, 3, dan 4 maka *traffic* 1 akan menempati slot 1, *traffic* 3 akan menempati slot 2 dan seterusnya. Pada Gambar 2.2 ditunjukkan mekanisme *Fixed TDM* pada sebuah *switch*. Pada berbasis SCN, forwarding *traffic* dilakukan dengan memetakan sebuah aliran *traffic* ke sebuah tabel yang berisi informasi input port, input slot, output port dan output slot. Sebagai contoh pada Gambar 2.2, *traffic* pada input port 1 pada slot 5 akan diteruskan ke output port 2 slot 4.

Penerapan *Fixed TDM* menjadikan SCN dapat memberikan kepastian *QoS* pada layanan komunikasi dikarenakan dengan alokasi waktu yang tetap dan terbatas pada kanal komunikasi untuk *Call Setup* yang sudah terbangun. *Fixed TDM* menjadi tidak efektif jika digunakan untuk melewatkan *traffic* internet yang bersifat *bursty* dan *multirate*.



Gambar 2.2. *Fixed Synchronous Multiplexer* [22]

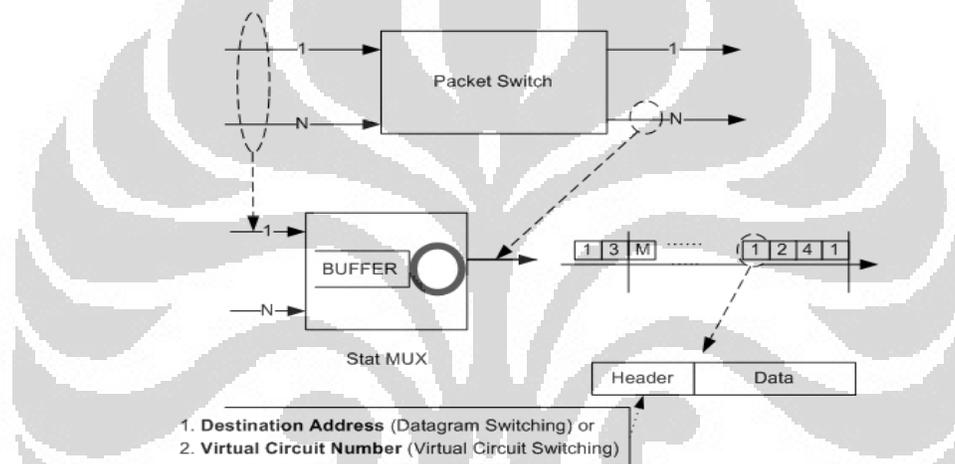
### 2.1.2. *Multiplexing* pada *Packet Switched Network*

Pemanfaatan infrastruktur jaringan yang sama untuk layanan suara, gambar dan data merupakan strategi yang digunakan oleh penyedia layanan telekomunikasi. Perkembangan jaringan dan layanan internet menjadi pendorong penyedia layanan telekomunikasi untuk memilih infrastruktur berbasis *Packet Switch Network* sebagai infrastruktur layanan.

Mekanisme multiplexing berbasis statistik digunakan pada jaringan *Packet Switched Network* ditunjukkan pada Gambar 2.3. Pada *Statistical Multiplexing* alokasi slot dalam *frame* pada pengiriman *traffic* tidak dilakukan secara tetap, *traffic* dipecah-pecah dalam paket yang diberi *header* informasi tujuan paket dan ditempatkan pada slot dalam *frame* melalui penjadwalan yang diatur oleh *Scheduler*. Sebuah buffer digunakan untuk menampung *traffic* dari masukan yang kemudian harus melalui sebuah *Scheduler* untuk diteruskan ke kanal keluaran.

Mekanisme *buffering* dan penjadwalan terhadap paket berpengaruh adanya keterlambatan pada paket yang dinamakan *Queuing Delay*. Jika kanal keluaran terutilisasi penuh, maka mekanisme *Packet Dropping* akan diterapkan pada paket yang memiliki prioritas terendah.

Mekanisme *Statistical Multiplexing* memberikan efisiensi yang baik pada penggunaan kanal komunikasi untuk melewati *traffic* internet yang memiliki karakteristik *bursty* dan *multirate*, namun kurang begitu baik dalam melayani *traffic* layanan yang bersifat *realtime* dikarenakan pengaruh *Queuing Delay* dan mekanisme *Packet Drop*.



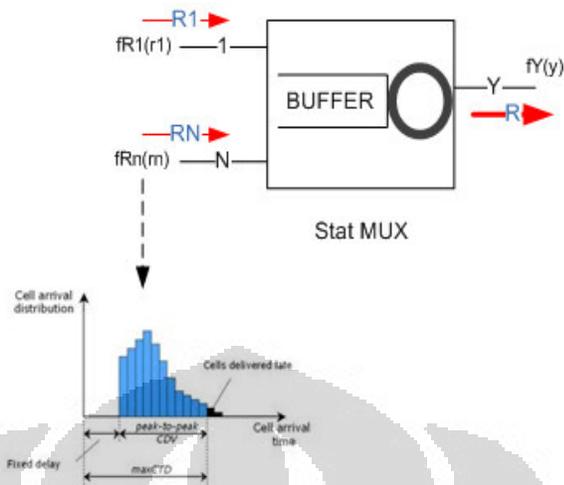
Gambar 2.3. Statistical Multiplexing [22]

### 2.1.3. Hipotesa Mekanisme *Admission Control*

*Admission Control* adalah mekanisme pengontrolan paket forwarding yang diterapkan pada *Statistical Multiplexer*. Pada *Packet Switched Network multiplexing* paket masukan untuk diteruskan ke kanal keluaran dapat diteruskan atau di drop. Kondisi yang menjadikan *multiplexer* melakukan drop paket dijelaskan pada hipotesa mekanisme *admission control* berikut:

Pada Gambar 2.4, jika masukan multiplexer adalah  $R_1, R_2 \dots R_n$ , maka *bit rate* keluaran sistem  $Y$  adalah penjumlahan dari semua masukan  $R_1, R_2 \dots R_n$

$$Y = R_1 + R_2 + \dots + R_n \quad (2.1)$$



Gambar 2.4. Hipotesa Admission Control [22]

Kondisi *traffic* pada masukan R1 merupakan fungsi dari kemungkinan kepadatan (*probability density function*)  $f_{R1}(r1)$  kanal komunikasi R1

$$R1 = f_{R1}(r1) \quad (2.2)$$

Kondisi *traffic* pada keluaran Y merupakan fungsi dari kemungkinan kepadatan jaringan  $f_Y(y)$

$$Y = f_Y(y) \quad (2.3)$$

Kondisi kepadatan jaringan kanal keluaran  $f_Y(y)$  dikatakan masih bisa meneruskan paket hingga nilai *traffic* keluaran Y lebih besar dari kapasitas bandwidth keluaran R, namun masih dibawah batas paket loss yang bisa ditoleransi  $\delta$

$$f_Y(y) = \text{Prob}[Y > R] \leq \delta \quad (2.4)$$

Jaringan dikatakan tidak memiliki keterlambatan dan loss jika jumlah puncak *traffic* (P) dari semua masukan masih dibawah kapasitas kanal R. Pada kondisi ini *traffic* dilayani dengan kualitas seperti pada *Switched Circuit Network*.

$$P1 + P2 + \dots + Pn \leq R \quad (2.5)$$

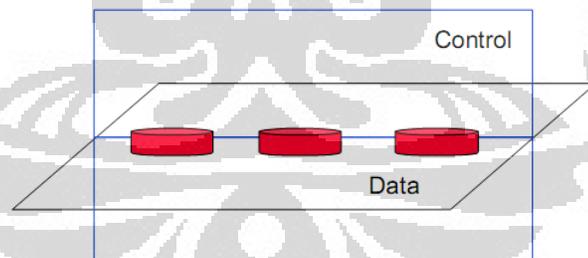
## 2.2. Manajemen Sumber Daya dan QoS

Pada jaringan berbasis *Packet Switched Network* terdapat beberapa skenario untuk dapat memberikan layanan yang optimal dan menjaga *QoS* pada layanan. Pendekatan yang dilakukan adalah dengan memberikan *resource link* dan ketersediaan yang dibutuhkan oleh *traffic* layanan. Penerapan *QoS* pada paket network dibutuhkan untuk menjawab kondisi pelayanan *traffic* pada *internet* dilakukan secara *Best Effort*, sedangkan tipe aplikasi dan pemilik dari *traffic* yang menggunakan internet memiliki kelas layanan yang berbeda.

### 2.2.1. Integrated Service

*Integrated service* adalah skenario *QoS* yang dirancang untuk digunakan pada integrasi layanan *real-time* pada jaringan *internet*. Jaminan *QoS* diterapkan dalam basis *per-flow*. *Integrated Service* memiliki kemampuan untuk pengalihan *traffic* tanpa memutus sesi komunikasi yang telah terjadi.

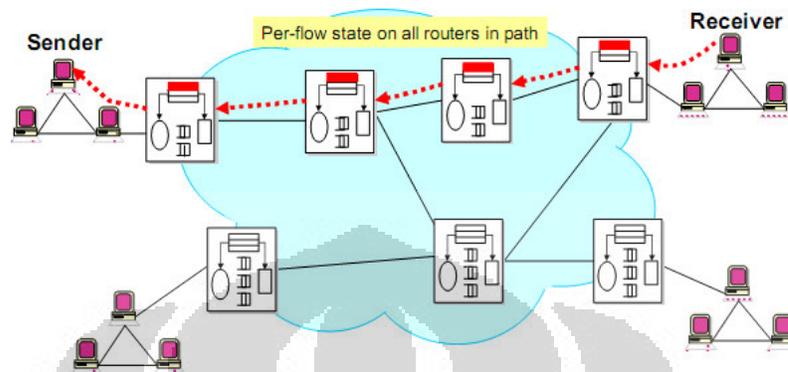
Pada *Integrated Service* ada dua hal yang dikontrol yaitu bagaimana informasi reservasi *resource* sampai ke *Router* (*Control Plane*), dan apa yang harus dilakukan pada paket data oleh *Router* (*Data Plane*) ditunjukkan pada Gambar 2.5.



Gambar 2.5. *Control Plane* dan *Data Plane* pada *IntServ* [22]

*Resource Reservation* adalah *Control Plane* yang dikirimkan oleh sumber *traffic* (pengirim), sedangkan *Admission Control* adalah *Control Plane* yang dikirimkan oleh tujuan *traffic* (penerima) *per-flow* pada setiap *Router* yang dilalui (Gambar

2.6). *Data Plane* pada *IntServ* menerapkan klasifikasi *per-flow* dan *scheduling* pada tiap *Router*.



Gambar 2.6. *Admission Control* pada *IntServ* [22]

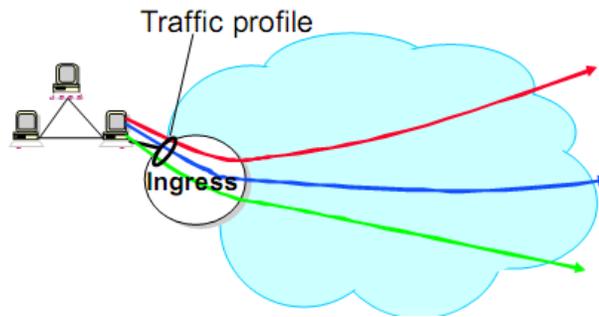
Mekanisme manajemen sumber daya jaringan berbasis *per-flow* pada *IntServ* menjadikannya sulit untuk diterapkan pada jaringan dengan skala besar seperti *internet*. Dari sisi ekonomi ini menimbulkan model pembiayaan yang rumit untuk interkoneksi antar operator.

### 2.2.2. *Differentiated Service*

*Differentiated Service (DiffServ)* memberikan layanan *QoS* dengan karakteristik Isolasi *QoS* per Agregate sehingga kepastian *QoS* layanan adalah per-aggregate dan cakupan layanan adalah dalam cakupan domain.

Pada *DiffServ Router Edge* memelihara *state* per-aggregate (Gambar 2.7), sedangkan *Router Core* memelihara lebih sedikit kondisi klas-kelas dari *traffic*.

Kepastian *QoS* pada implementasi *DiffServ* lebih rendah dari pada *IntServ* dikarenakan penerapan pada level aggregate dibanding dengan penerapan per-flow.



Gambar 2.7. Profiling *traffic* dilakukan oleh *Edge Router* [22]

## 2.3. Tinjauan Umum NGN

Teknologi berbasis NGN diterapkan dengan mengacu pada arsitektur dan protokol berbasis SIP. Arsitektur yang ada pada saat ini juga telah mempersyaratkan penerapan QoS.

### 2.3.1. Arsitektur NGN

Arsitektur fungsional NGN TISPAN (Gambar 2.8) dibangun dengan mengacu pada *Service Layer* dan *Transport Layer* berbasis IP.

*Service Layer* pada arsitektur NGN TISPAN terdiri dari:

- Komponen *IP Multimedia Core Subsystem* (IMS)
- *PSTN/ISDN Emulation Subsystem* (PES)
- Subsistem multimedia lain
- Komponen umum yang dibutuhkan, seperti untuk pengaksesan aplikasi, fungsi *charging* dan lainnya

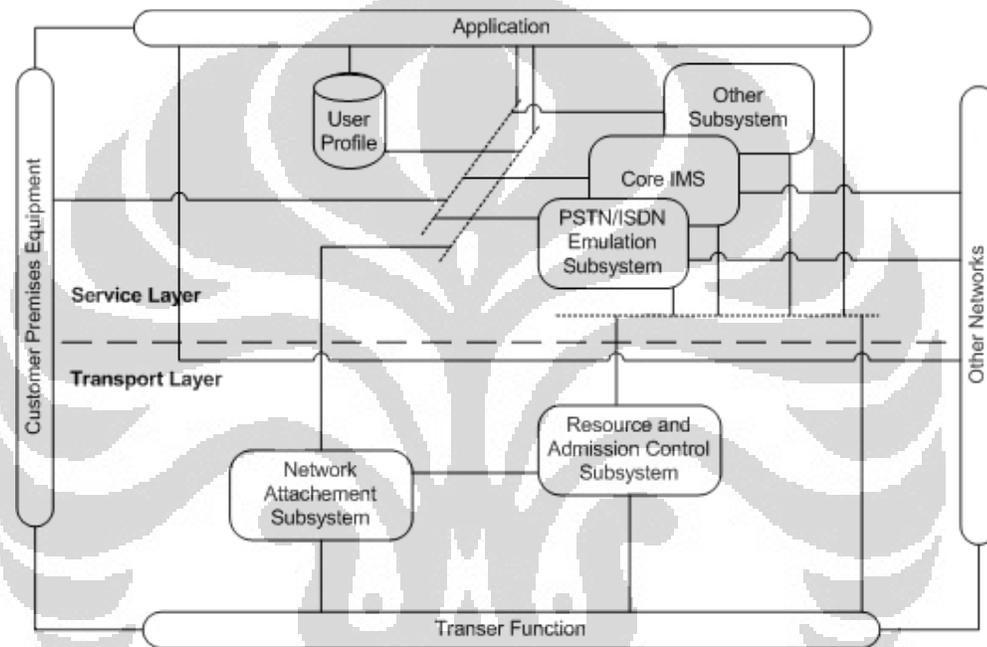
*Transport Layer* pada arsitektur NGN TISPAN terdiri dari:

- *Resource and Admission Control Subsystem* (RACS)
- *Network Attachment Subsystem* (NASS)

Interkoneksi IP digunakan oleh perangkat pengguna (*User Endpoint*) pada *Transport Layer* dengan pengontrolan yang dilakukan oleh NASS dan RACS. Subsistem ini mencakup teknologi dibawah *layer* IP, yang digunakan pada *Access Network* dan *Core Network*.

NGN *IP Multimedia Subsystem* (IMS) menggunakan pensinyalan berbasis protokol SIP untuk melakukan *provisioning* terhadap layanan-layanan multimedia yang menginterkoneksi antara terminal pengguna, *server* aplikasi, *server* media dan *IP Multimedia Gateway*.

NGN IMS memiliki kemiripan fungsi dengan entitas pada 3GPP IMS, variasi yang ada dikarenakan perbedaan pada Access Network dan tipe dari perangkat pengguna.

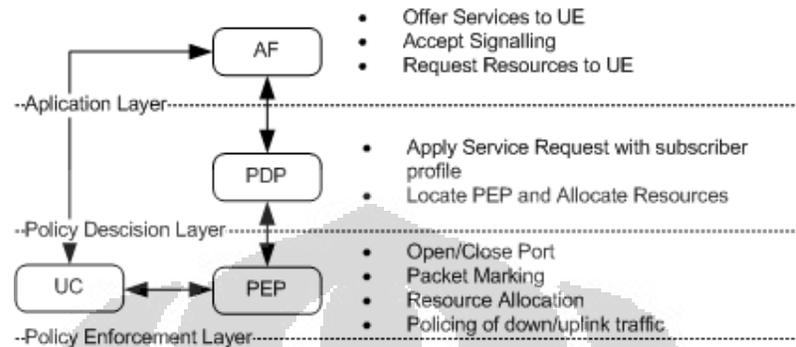


Gambar 2.8. Arsitektur menyeluruh NGN TISPAN [20]

### 2.3.2. Penerapan QoS pada NGN

Penerapan *QoS* pada layanan jaringan berbasis IP dapat mengacu pada arsitektur *Policy Based Admission Control* yang didefinisikan oleh IETF (Gambar 2.9). Pada arsitektur ini, *Application Function* (AF) diposisikan SIP *Server* yang menjadi tujuan pensinyalan SIP dan mengakses informasi terkait permintaan layanan dan informasi detail terkait media. Selanjutnya AF akan melakukan *query* dan memberikan informasi terkait ke *Policy Decision Point* (PDP). PDP akan memutuskan apakah permintaan layanan diteruskan atau ditolak berdasarkan kebijakan, informasi permintaan dan profile pengguna. Pada kondisi pemberian

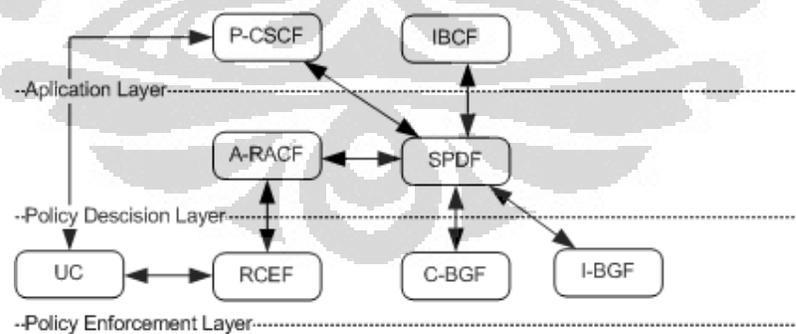
akses pada layanan, PDP akan mengirimkan informasi terkait aturan yang harus diterapkan pada Policy Enforcement Point (PEP) [21].



Gambar 2.9. IETF Architecture of Policy Based Admission Control

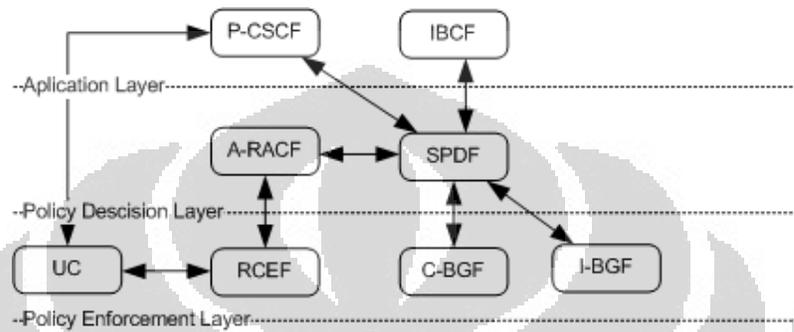
Badan standarisasi 3GPP (*Mobile Network*) dan ETSI TISPAN (*Fixed NGN Network*) telah merancang arsitektur penerapan *QoS* pada NGN yang didasari pada kebutuhan *Access Network* yang berbeda.

Pada 3GPP arsitektur ini dinamakan *Policy and Charging Control* (PCC), Gambar 2.10 memetakan fungsi utama dari PCC ke fungsi dan layer pada arsitektur *Policy Based Admission Control* IETF.



Gambar 2.10. 3GPP PCC Architecture

ETSI-TISPAN mendefinisikan arsitektur yang terkait dengan penerapan *QoS* pada NGN IMS yang dinamakan *Resource and Admission Control Subsystem (RACS)*, Gambar 2.11 memetakan fungsi utama dan layer RACS pada *Policy Based Admission Control IETF*.



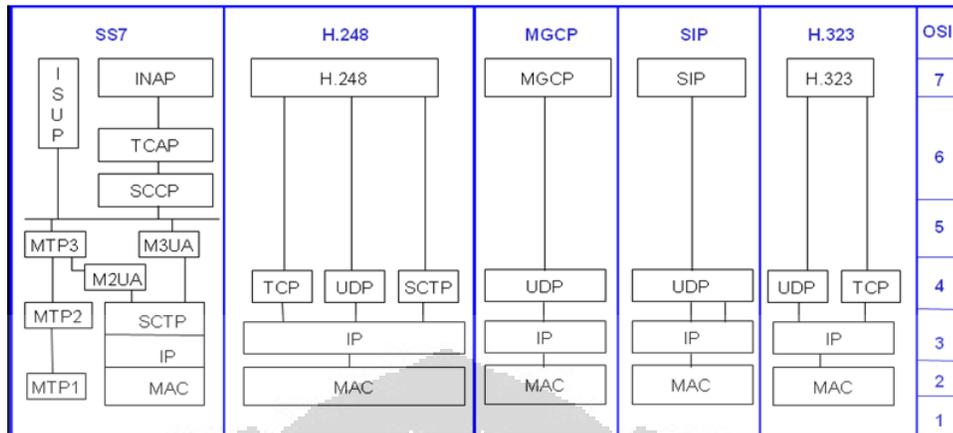
Gambar 2.11. ETSI TISPAN RACS Architecture

### 2.3.3. Klasifikasi Protokol NGN

*Next Generation Network* menggunakan berbagai protokol untuk interkoneksi antar komponen yang ada baik antar perangkat maupun komunikasi antar pengguna. Secara umum protokol-protokol ini dikelompokkan menjadi tiga golongan yaitu *Signalling Transport Protocol*, *Bearer Control Protocol*, *Call Control Protocol* [2].

- *Signalling Transport Protocol* melayani signalling pada layer transport dalam melewatkan layanan yang berjalan di atasnya.
- *Bearer Control Protocol* berfungsi untuk pengontrolan media gateway yang ada pada NGN.
- *Call Control Protocol* digunakan untuk mengontrol setup panggilan yang ada pada layanan telekomunikasi.

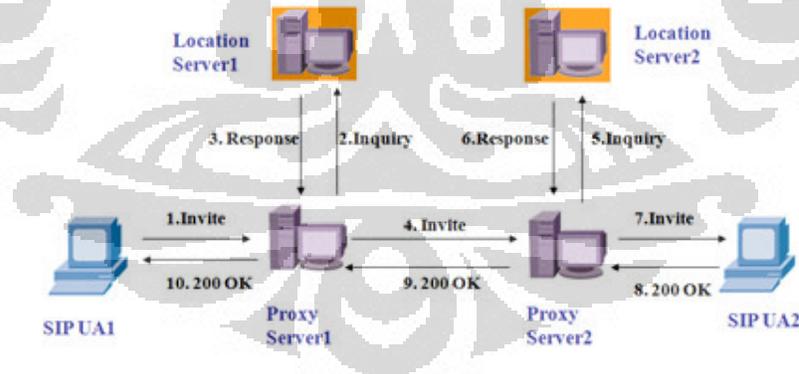
Susunan protokol-protokol yang digunakan pada NGN dijelaskan pada Gambar 2.12.



Gambar 2.12. Protokol NGN [2]

## 2.4. Prinsip Protokol Session Initiation Protocol (SIP)

*Session Initiation Protocol* adalah protokol yang digunakan untuk membuat, merubah dan memutuskan sesi-sesi pada satu atau lebih partisipan. [4]. SIP merupakan protokol utama IETF untuk arsitektur kontrol multimedia dan data.



Gambar 2.13. Komunikasi SIP [3]

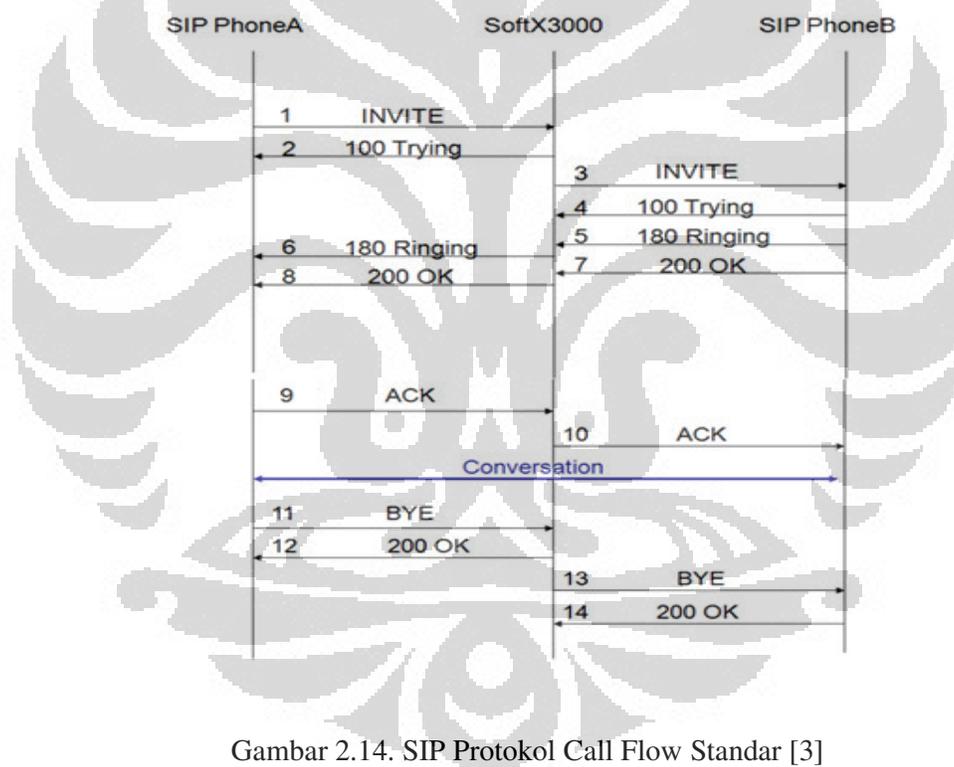
Pada SIP didefinisikan entitas-entitas sesuai Gambar 2.13 sebagai berikut:

- *Location Service*
- *Proxy Server*

- *Redirect Server*
- *Registrar*
- *User Agent (Client and Server)*

SIP memiliki 2 tipe pesan yaitu pesan *Request* dan pesan *Response*. Pesan *Request* merupakan pesan yang dikirimkan dari *client* ke *server*. Meliputi pesan *INVITE*, *ACK*, *BYE*, *CANCEL*, *REGISTER*, *OPTION*. Pesan *Response* digunakan untuk menampilkan respon dari *server* terhadap *Request* dari *client*. Meliputi respon 1xx, 2xx, 3xx, 4xx, 5xx and 6xx and *ACK*

Proses *Call Setup* dan *Teardown* pada signaling dengan protokol SIP secara umum sesauai dengan *Call Flow* pada Gambar 2.14.



Gambar 2.14. SIP Protokol Call Flow Standar [3]

## 2.5. Implementasi Manajemen *Traffic* pada *Linux*

Kemampuan sistem operasi linux yang memiliki fitur yang bisa di optimalkan menjadi network operating sistem untuk digunakan sebagai *Router* dalam infrastruktur jaringan. Penggunaan linux sebagai *Router* memberikan kemungkinan yang luas pada kustomisasi topologi dan layanan jaringan dengan

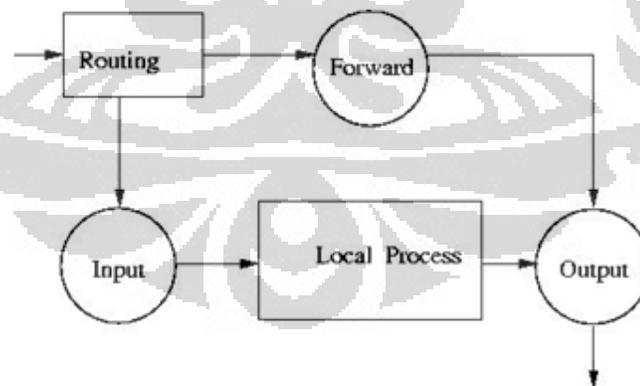
banyaknya fitur-fitur yang dikembangkan oleh komunitas *Open Source*. Kemudahan pengaksesan dan ikut serta dalam pengembangan fitur menjadi salah satu faktor pesatnya perkembangan teknologi berbasis linux.

*Traffic Control* merupakan salah satu fitur yang diimplementasikan pada teknologi linux. Beberapa implementasi *Traffic Control* yang digunakan secara luas adalah manajemen *QoS*, *Traffic Marking* dan *Filtering* serta *Policy Routing*

### 2.5.1. Packet Filtering Firewall

*Packet Filtering Firewall* adalah perangkat lunak yang dalam operasinya mengamati header dari aliran paket, yang selanjutnya akan menentukan diteruskan atau tidaknya paket tersebut atau kemungkinan dilakukan implemmentasi lain dengan aksi yang lebih kompleks. Pada sistem Linux, *Packet Filtering* dibangun didalam *corelinux* fitur kernel routing pada sub seksi firewall.

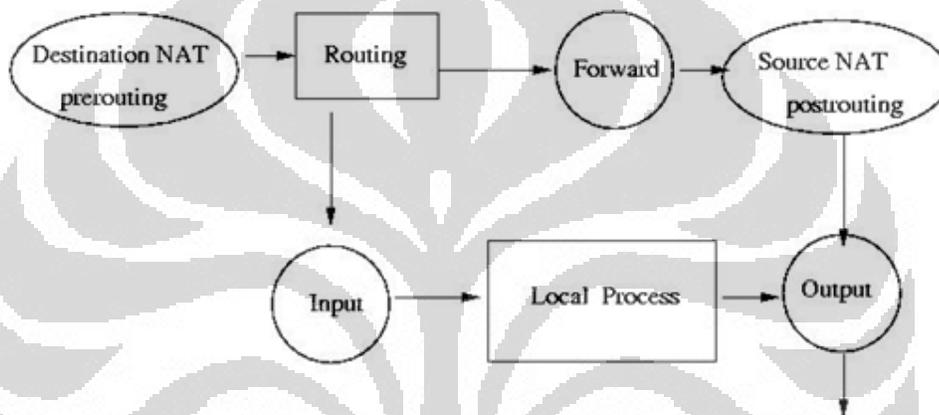
Salah satu perangkat lunak *packet filtering firewall* adalah *Netfilter/iptables*. *Iptables* terdiri dari dua komponen yang terpisah yaitu *kernel-space module* yang terdistribusi pada kernel utama linux dan *user-space tools* berbentuk aplikasi binary bernama 'iptables' yang didistribusikan terpisah dari *kernel tree* utama.



Gambar 2.15. Operasi *Forwarding* Netfilter/IPTABLE [11]

*Iptables* memiliki tiga tabel yang diperuntukan untuk tiga operasi yang berberda sebagai berikut:

- *Filtering*, merupakan tabel yang digunakan untuk operasi yang menentukan apakah trafik diteruskan atau di block. Aliran pemrosesan paket ditunjukkan pada Gambar 2.15.
- *Mangle*, digunakan untuk merubah field tertentu pada *header* paket IP.
- *Network Address Translation (NAT)*, digunakan untuk mentranslasi *field* informasi alamat IP asal dan alamat IP tujuan pada paket IP. Aliran pemrosesan paket pada operasi ini ditunjukkan pada Gambar 2.16.



Gambar 2.16. Operasi NAT Netfilter/IPTABLE [11]

### 2.5.2 Policy Routing

Implementasi penentuan *routing* umumnya ditentukan oleh alamat tujuan paket, yang dicocokkan dengan informasi alamat network dan *gateway* terkait yang berada dalam tabel *routing* pada *Router*.

*Policy Routing* adalah operasi *routing* paket yang tidak hanya berdasarkan alamat IP tujuan, namun juga berdasarkan alamat IP asal, protokol IP, port pada protokol *transport*, atau bahkan *payload* dari paket. Pada sistem Linux, *Policy Routing* mengganti penggunaan *routing table* konvensional dengan sebuah *database* yang dinamakan *Routing Policy Database (RPDB)* yang memilih *route* berdasarkan eksekusi pengecekan beberapa set aturan (*Policy Routing Rule*) [12].

Setiap *Policy Routing Rule* (PRR) memiliki *Selector* dan *Action Predicate*. Dalam penentuan set PRR yang cocok, PRDB dipindai secara inkremental. Pada saat startup, kernel akan mengkonfigurasi standar RPDB yang berisi tiga set aturan pada Tabel 1.

Table 1. Kebijakan default Policy Routing [12]

Priority	Selector	Action
0	match anything	lookup routing table local (ID 255)
32766	match anything	lookup routing table main (ID 254)
32767	match anything	lookup routing table default (ID 253)

### 2.5.3. Traffic Control

*Traffic Control* adalah salah satu fitur manajemen *traffic* yang telah diimplementasikan pada *kernel Linux*.

#### 2.5.3.1. Operasi

*Traffic Control* meliputi operasi sebagai berikut [7]:

- *Shapping*, merupakan operasi yang ditujukan untuk mengontrol *rate* transmisi dari *traffic*. Operasi *shapping* terjadi pada aliran *traffic* ke arah luar (*egress*).
- *Scheduling*, operasi ini meliputi proses *reordering* dan prioritasasi yang terjadi pada *egress*. *Scheduling* diperlukan untuk memastikan ketersediaan *bandwith* bagi *bulk trasnfer*.
- *Policing*, Merupakan operasi yang ditujukan untuk menerapkan kebijakan pada paket yang datang. *Policing* terjadi pada *traffic incoming* (*ingress*)
- *Dropping*, merupakan proses untuk tidak meneruskan paket (*dropped*), hal ini terjadi apabila *traffic* telah melebihi *bandwitdh* yang ditentukan.

### 2.5.3.2. Object pengontrol pemrosesan *traffic*

Pemrosesan *traffic* dikontrol oleh tiga objek sebagai berikut [7]:

- *QDISCS*, merupakan singkatan dari *queueing discipline*. Merupakan hal dasar dalam memahami *Traffic Control*. Ketika *kernel* akan mengirimkan paket ke arah *interface*, paket terlebih dulu di antrikan dalam *qdisc* yang dikonfigurasi pada *interface* tersebut. Selanjutnya *kernel* akan mengambil sebanyak mungkin paket-paket dari *qdisc*, dan mengirimkannya ke *driver network adapter*.
- *CLASSES*, beberapa *qdisc* berisi kelas-kelas, yang berisi *qdisc* selanjutnya. *Traffic* dapat diantrikan dalam *inner-qdisc* yang berada didalam kelas. Sebagai contoh, *qdisc* dapat memprioritaskan *traffic* tertentu dengan cara mendahulukan *dequeue traffic* dari kelas tertentu dibanding dengan kelas yang lain.
- *FILTERS*, adalah salah satu metode klasifikasi yang digunakan untuk menentukan paket mana yang akan di antrikan. *Traffic* yang datang akan dicocokkan dengan kelas dan sub-kelas yang ada hingga didapatkan keputusan dimana *traffic* akan ditempatkan. Jika tidak ada satupun kriteria yang sesuai, maka kriteria baru akan dibuat.

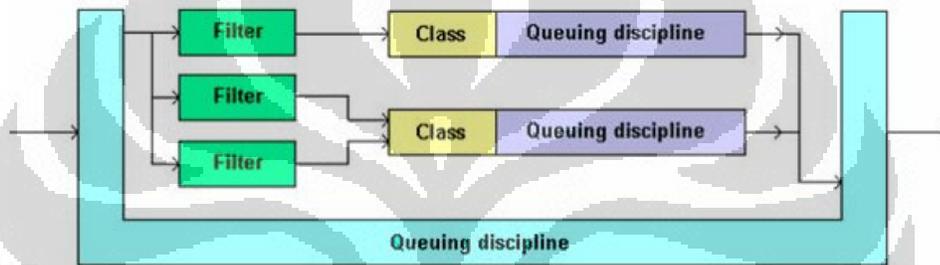
### 2.5.3.3. Disiplin antrian

Disiplin antrian di kategorikan menjadi *Classful Queuing Disciplines* dan *Classless Queuing Disciplines*.

- *Classful Queuing Disciplines* memiliki filter-filter yang memungkinkan paket-paket untuk diarahkan ke kelas dan sub-antrian tertentu. *Classful qdisc* sangat berguna untuk menerapkan kebijakan penanganan yang berbeda berdasarkan tipe *traffic*. Proses *Classful qdisc* ditunjukkan pada Gambar 2.17. Termasuk dalam kategori ini adalah *qdisc* berikut:
  1. *Class Based Queueing CBQ qdisc*
  2. *Hierarchy Token Bucket, HTB qdisc*
  3. *PRIQ qdisc*
- *Classless Queuing Disciplines* adalah *qdisc* yang menerima paket dan hanya dapat melakukan penjadwalan ulang, menunda atau men-*drop*

*traffic*. Classless disc dapat digunakan untuk men-*shape* traffik untuk interface secara keseluruhan. *Qdisc* ini bisa digunakan sebagai *qdisc* utama pada *interface*, atau digunakan didalam *leaf-class* sebuah *Classfull qdisc*. Termasuk dalam kategori ini adalah *qdisc* berikut:

1. *[plb]fifo*, *pure First In, First Out behaviour*.
2. *pfifo\_fast*, *Standard qdisc for Advanced Router enabled kernels*.
3. *red*, *Random Early Detection*
4. *sfq*, *Stochastic Fairness Queueing*
5. *tbq*, *The Token Bucket Filter*



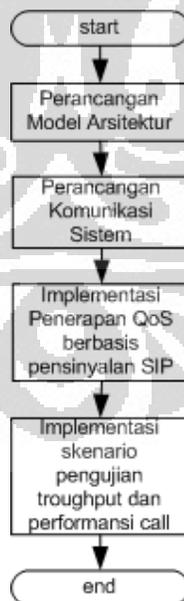
Gambar 2.17. *Classful Queuing Disciplin* [7]

## BAB 3 PERANCANGAN DAN IMPLEMENTASI

### 3.1. Skenario Perancangan

Sistem yang dirancang diharapkan dapat memberikan layanan pengaksesan jaringan melalui mekanisme otentikasi tunggal berbasis protokol SIP untuk layanan *voice*, *video* dan data. Proses lebih lanjut terkait dengan otorisasi aplikasi dan penyediaan jalur komunikasi yang dibutuhkan, dilakukan oleh proses-proses yang transparan dari sisi pengguna.

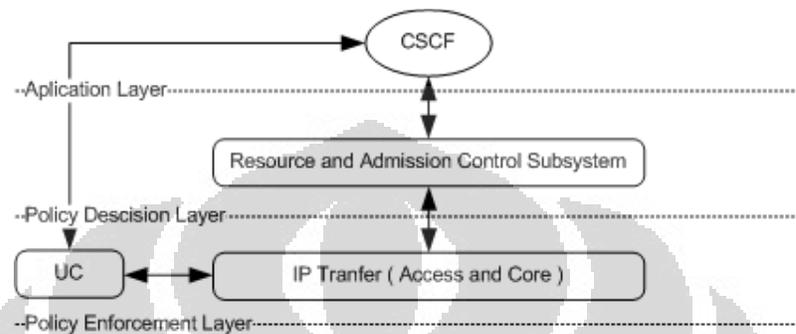
Pada kegiatan tesis ini difokuskan pada perancangan penerapan *QoS* dan pengontrolan keberhasilan panggilan SIP berdasarkan ketersediaan sumberdaya jaringan. Kegiatan tersebut memerlukan kegiatan perancangan pemodelan lain yang diluar fokus kegiatan perancangan utama. Perancangan pemodelan tersebut adalah perancangan fungsi pada model arsitektur jaringan dengan kebijakan *QoS* yang dinamis, perancangan modifikasi protokol *Call Establishment* berbasis SIP serta skenario pengujian yang mengukur performansi *Call* dan utilisasi bandwidth jaringan. *Flow Chart* kegiatan perancangan ditunjukkan pada gambar 3.1.



Gambar 3.1. Flowchart kegiatan perancangan

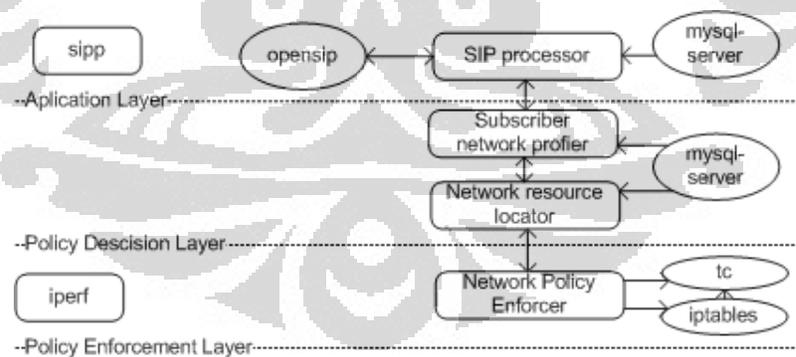
### 3.2. Arsitektur Rancangan

Sistem kontrol pengaksesan jaringan dan penerapan *QoS* berbasis *SIP* yang dibangun mengacu pada fungsi arsitektur *Policy Based Admission Control* yang didefinisikan oleh IETF.



Gambar 3.2. Pemetaan rancangan terhadap subsistem NGN

Kesesuaian terhadap arsitektur yang didefinisikan oleh ETSI TISPAN (Gambar 3.2) dilakukan dengan memetakan fungsi-fungsi yang dibangun dengan komponen yang meliputi *Call Session Control Function* (CSCF) pada Service Layer NGN IMS dan *Resource and Admission Control Subsystem*, dan *IP Transfer* pada Transport Layer NGN IMS.



Gambar 3.3. Diagram fungsi pada rancangan arsitektur

Arsitektur fungsional (Gambar 3.3) dari sistem yang dibangun meliputi:

- *SIP Processor* yang berfungsi untuk memproses lebih lanjut pesan-pesan SIP yang diterima oleh *SIP Server* dan memetakan informasi terkait

alamat *IP caller* dan *callee* pada sebuah *call request*, maupun alamat IP terminal pada sesi registrasi pengguna SIP.

- *Subscriber Network Profiler* memetakan informasi pengguna yang terkait dengan penerapan kebijakan pengaksesan jaringan dan pengaksesan layanan, hal ini meliputi diantaranya adalah profil *QoS*
- *Network Resource Locator*, memetakan lokasi dari terminal pengguna dan memetakan perangkat pada layer transport yang relevan dengan penerapan kebijakan jaringan terkait dengan sesi panggilan maupun sesi registrasi.
- *Network Policy Enforcer* menerapkan aturan (rule) dari kebijakan pengaksesan jaringan dan layanan (policy)

### 3.3. Komponen

Komponen pada perancangan dijelaskan sebagai berikut.

#### 3.3.1. *Call Session Control Function (CSCF)*

Komponen CSCF menyediakan layanan *signaling* berbasis SIP yang memproses layanan komunikasi multimedia dan registrasi bagi terminal pengguna. Pada arsitektur yang dibangun, CSCF juga memiliki fungsi sebagai *SIP Processor*. CSCF meng-ekstrak informasi yang dibutuhkan oleh *Policy Decision Point (PDP)* terkait identifikasi pengguna dan alamat IP yang digunakan oleh pengguna. Dalam konteks registrasi terminal, CSCF mengekstrak informasi IP terminal yang digunakan. Dalam konteks *Call Setup* dan *Teardown*, CSCF mengekstrak informasi identifikasi *Caller* dan *Callee*, serta alamat IP yang digunakan oleh terminal *Caller* dan *Callee*.

Informasi hasil ekstraksi pesan SIP oleh CSCF kemudian dikirimkan ke komponen *Policy Decision Point*. Pada kegiatan tesis ini, komunikasi antara CSCF dan *Policy Decision Point* dilakukan dengan menggunakan jalur berbasis Web Service.

### 3.3.2. *Policy Decision Point (PDP)*

Analisa terhadap permintaan penerapan kebijakan pengaksesan jaringan dan layanan dilakukan pada *Policy Decision Point (PDP)* dengan *query* database pada profil pengguna yang dilakukan oleh fungsi *Subscriber Network Profiler (SNP)* untuk mendapatkan informasi diantaranya mengenai alokasi *bandwidth* untuk layanan IP dan *bandwidth* spesifik untuk mentransmisikan paket *realtime multimedia*.

Informasi alamat IP terminal digunakan oleh *Network Resource Locator (NRL)* untuk mendapatkan alamat *network* dan *IP Gateway* dimana terminal berada. Informasi yang didapatkan dari fungsi SNP dan NRL selanjutnya menjadi acuan olah PDP untuk mengirimkan instruksi penerapan *QoS* sesuai dengan alokasi *bandwidth* untuk pengguna pada *Gateway* yang berperan sebagai *Policy Enforcement Point*.

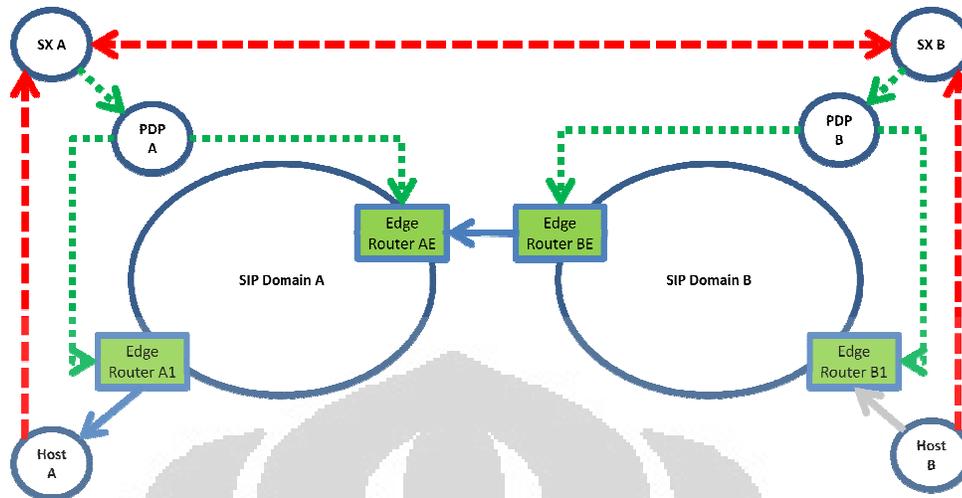
Pada kegiatan tesis ini, komunikasi antara *Policy Decision Point* dan *Policy Enforcement Point* dilakukan dengan menggunakan jalur berbasis *Web Service*.

### 3.3.3. *Policy Enforcement Point (PEP)*

Penerapan aturan pada kebijakan pengaksesan jaringan dan layanan dilakukan pada *Policy Enforcement Point (PEP)*. Komponen PEP pada kegiatan ini menerapkan QoS dengan menggunakan solusi berbasis *opensource*. Aplikasi berbasis *kernel linux Traffic Controller (TC)* dan *IPTABLES*.

### 3.4. Penerapan QoS berbasis SIP

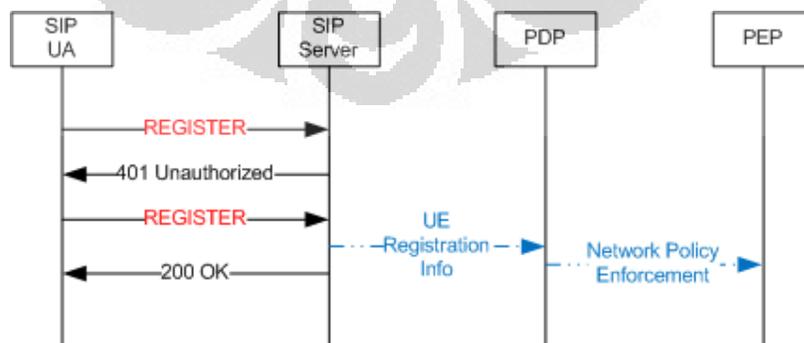
Pada implementasinya, arsitektur memanfaatkan pensinyalan berbasis SIP untuk penerapan QoS (garis panah putus-putus) untuk memicu proses kontrol (panah titik putus-putus), yang mengatur QoS trafik yang dilewatkan pada jaringan (panah garis solid), yang ditunjukkan pada gambar 3.4.



Gambar 3.4. Diagram Penerapan QoS berbasis SIP

### 3.4.1. Registrasi SIP UA

Pada implementasi ini kejadian sukses registrasi dan sukses deregistrasi terminal pengguna akan memicu proses penerapan aturan kebijakan alokasi *bandwidth* untuk tiap pengguna yang teregistrasi. Alokasi *bandwidth* diterapkan untuk keseluruhan trafik IP, tidak terbatas pada aplikasi tertentu. Alokasi *bandwidth* juga dapat mempertimbangkan kemungkinan penggunaan lebih dari satu terminal oleh pengguna, yang melalui proses pengecekan terhadap status pengguna, dapat membatasi pengaksesan dengan mekanisme membagi penggunaan jaringan sesuai dengan profil alokasi *bandwidth* yang ditentukan. Fungsi penggunaan alokasi *bandwidth* untuk banyak terminal belum diterapkan pada saat kegiatan ini.

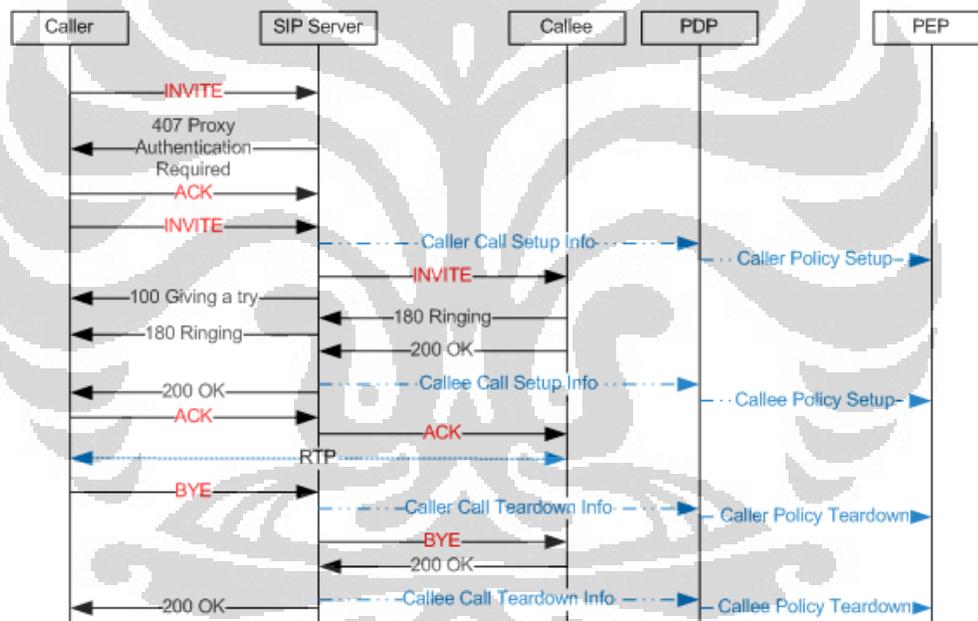


Gambar 3.5. Diagram komunikasi pada registrasi SIP UA

Dalam kasus deregistrasi terminal, sistem akan melepas reservasi alokasi *bandwidth*. Perbedaan kejadian registrasi dan deregistrasi adalah dengan menganalisa nilai *Expire* pada *header* pesan *REGISTER* SIP, proses deregistrasi ditunjukkan dengan nilai 0.

### 3.4.2. Call Setup dan Teardown

Mekanisme alokasi *bandwidth* secara dinamis diterapkan untuk memastikan *traffic* multimedia mendapatkan prioritas yang lebih ditinggi dari *traffic* IP lainnya dalam transfer data yang dilakukan oleh pengguna. Mekanisme ini tidak menambah jumlah alokasi *bandwidth* per-pengguna, namun hanya memberikan prioritas yang berbeda dalam alokasi *bandwidth* yang sudah ditentukan.



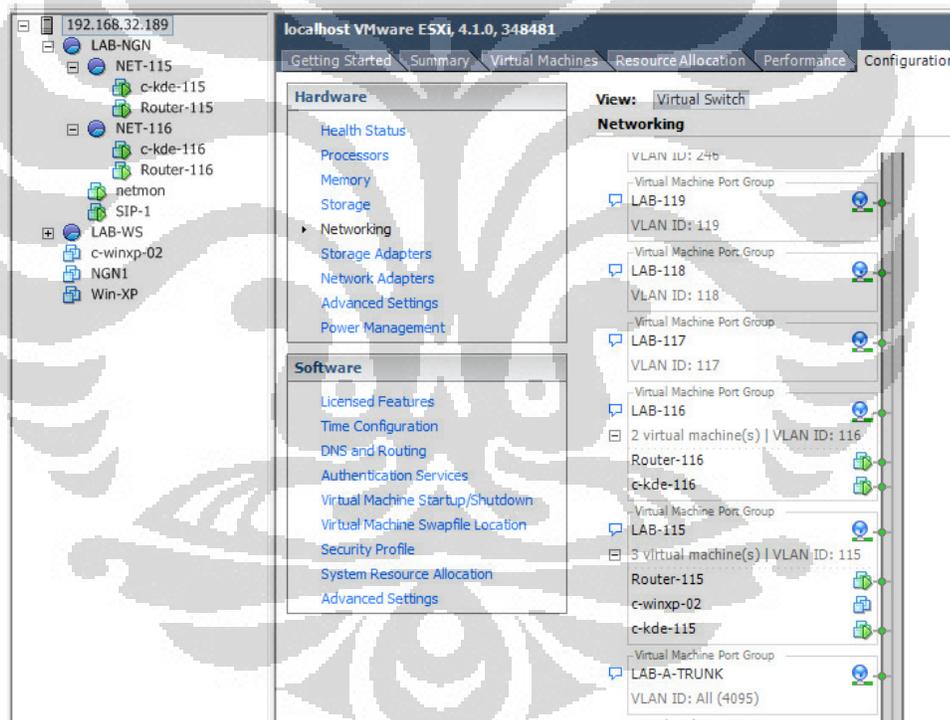
Gambar 3.6. Diagram komunikasi pada Call Setup and Teardown

*Call Setup* akan memicu *Policy Setup* pada kanal yang dialokasikan per-pengguna. Pesan *INVITE* yang ter-otentikasi akan memicu SIP Server untuk mengirimkan informasi identifikasi pengguna, alamat IP terminal dan informasi *codec* yang digunakan, serta *port* UDP yang ditawarkan untuk penerimaan paket multimedia *realtime* (RTP). Pada proses ini *Policy Setup* dilakukan pada kedua kanal komunikasi baik disisi *Caller* maupun *Callee*. *Policy Setup* di sisi *Callee* dipicu pada saat CSCF menerima pesan 200 OK dari sisi *Callee*.

*Call Teardown* terjadi pada saat salah satu dari partisipan *Call* mengirimkan pesan *BYE*, pada gambar 3.6, *Caller* memutuskan sesi panggilan dan mengirimkan pesan *BYE* yang diterima oleh CSCF. CSCF selanjutnya mengirimkan informasi ke PDP yang akan memicu instruksi melepas reservasi alokasi *bandwidth* pada PEP. *Policy Teardown* pada sisi *Callee* dipicu pada saat CSCF menerima pesan 200 OK dari sisi *Callee*, yang terkait dengan respon pesan *BYE* yang dikirimkan oleh *Caller*.

### 3.5. Infrastruktur Rancang Bangun

Infrastruktur kegiatan rancang bangun dan pengujian dilakukan dengan memanfaatkan teknologi berbasis linux.



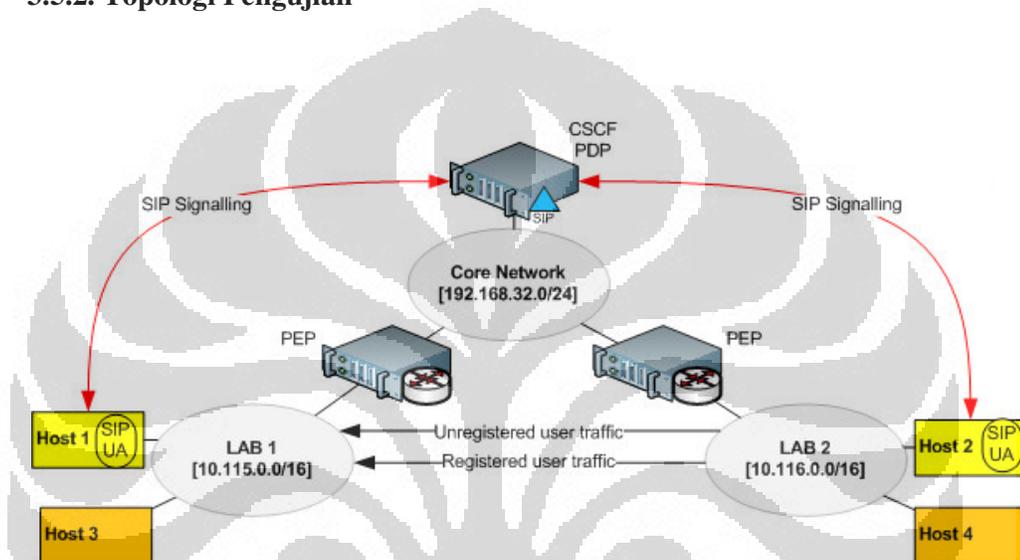
Gambar 3.7. Konfigurasi Lingkungan Pengujian Berbasis Virtualisasi

#### 3.5.1. Lingkungan Kerja Rancang Bangun

Pada kegiatan ini infrastruktur dibangun diatas lingkungan berbasis *Virtualisasi*. *Hypervisor Engine* ESX 4.0 di gunakan diatas mesin *Server IBM X*. Sebuah *Virtual Switch* dikonfigurasi untuk bisa menampung tiga *Virtual LAN*, 1 *Core*

*Network* dan 2 VLAN untuk *Node Client*. Pada kegiatan rancang bangun dan pengujian ini menggunakan lima mesin *virtual* (VM), 1 VM digunakan untuk CSCF dan PDP, 2 VM untuk PEP, dan 2 VM yang disimulasikan sebagai *User Endpoint* (UE). Gambar 3.7 menunjukkan tampilan *VM Manager* terkait dengan konfigurasi lingkungan rancang bangun.

### 3.5.2. Topologi Pengujian



Gambar 3.8. Konfigurasi Topologi Pengujian

Pengujian terhadap keberhasilan implementasi yang dilakukan pada kegiatan ini dilakukan dengan membagun topologi pengujian (Gambar 3.8). Sebuah *Server* yang berfungsi sebagai CSCF dan PDP, serta dua *Router* yang berfungsi sebagai PEP dihubungkan ke segmen *Core Network*, pada pengujian ini menggunakan segment IP 192.168.32.0/24. Dua segmen jaringan LAB difungsikan sebagai *Access Network*. LAB 1 menggunakan segmen 10.115.0.0/16, pada segmen ini dihubungkan sebuah VM yang difungsikan sebagai UE, yang diset untuk dapat mensimulasikan untuk 5000 terminal. LAB 2 menggunakan segmen 10.116.0.0/16, pada segmen ini dihubungkan sebuah VM yang difungsikan sebagai SIP *User Agent Server* dan *Application Server*.

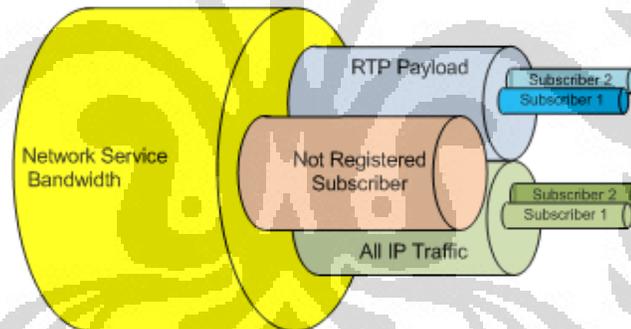
## BAB 4

### PENGUJIAN DAN ANALISA KINERJA

Penerapan kontrol pengaksesan jaringan dan penerapan *QoS* pada kegiatan ini meningkatkan fungsi kontrol pada pengelolaan jaringan dengan memberikan prioritas yang lebih tinggi pada pengguna yang melakukan registrasi, dan prioritas yang lebih tinggi lagi bagi *Realtime Traffic* multimedia pada sesi panggilan yang dilakukan oleh pengguna. Namun kemampuan ini memberikan pengaruh pada penurunan kinerja pada layanan *Call Control* CSCF, hal ini disebabkan adanya proses lebih jauh terkait dengan penerapan *Network Policy*.

Pada pengujian yang dilakukan akan diukur keberhasilan penerapan kontrol terhadap *throughput* dan pengaruh penurunan kinerja layanan *Call Control*.

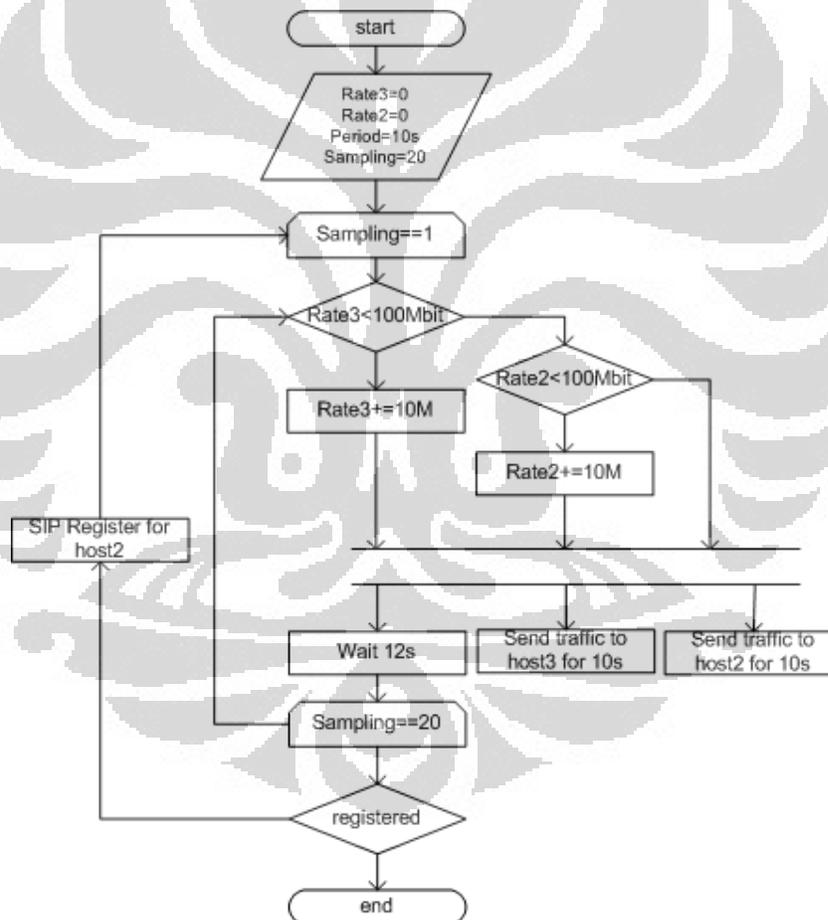
#### 4.1. Pengaruh Penerapan *QoS* pada *Traffic* Jaringan



Gambar 4.1. Skenario Penerapan *QoS*

*Interface* jaringan dari setiap mesin mendukung kecepatan hingga kecepatan 1Gbps. Namun untuk kegiatan pengujian ini kanal komunikasi dibatasi hingga kecepatan 100Mbps. Lebih lanjut kanal komunikasi ini dibagi menjadi tiga sub-kanal yaitu kanal 1 untuk pengguna yang tidak ter-registrasi, kanal 2 untuk pengguna yang melakukan registrasi dan kanal 3 untuk *traffic* multimedia *realtime*. Pada kanal 1, diterapkan kebijakan jaringan *default best effort*. Kanal 2 memiliki prioritas yang lebih tinggi dari kanal 1, pada saat pengguna melakukan registrasi maka akan terbentuk sub-kanal dengan alokasi maksimum *bandwidth*

sesuai dengan profil *QoS* yang diperuntukan hanya bagi spesifik bagi pengguna tersebut. Seiring dengan penambahan sub-kanal untuk pengguna, kapasitas kanal 2 akan membesar hingga maksimum memenuhi kapasitas kanal utama. Kanal 3 akan terbentuk jika ada *Call Session* yang dilakukan oleh satu atau lebih pengguna. Kanal 3 terbentuk dari sub-kanal sub-kanal yang spesifik terbentuk untuk *Call Session* dengan alokasi *bandwidth* yang sesuai dengan profil *codec* yang digunakan. Kanal 3 memiliki prioritas yang lebih tinggi dari semua kanal yang dibentuk untuk pengguna, sehingga dimungkinkan keseluruhan kanal utama digunakan oleh kanal 3 tanpa memberikan ruang pada kanal lainnya. Gambar 4.1 menggambarkan alokasi kanal pada skenario pengujian.



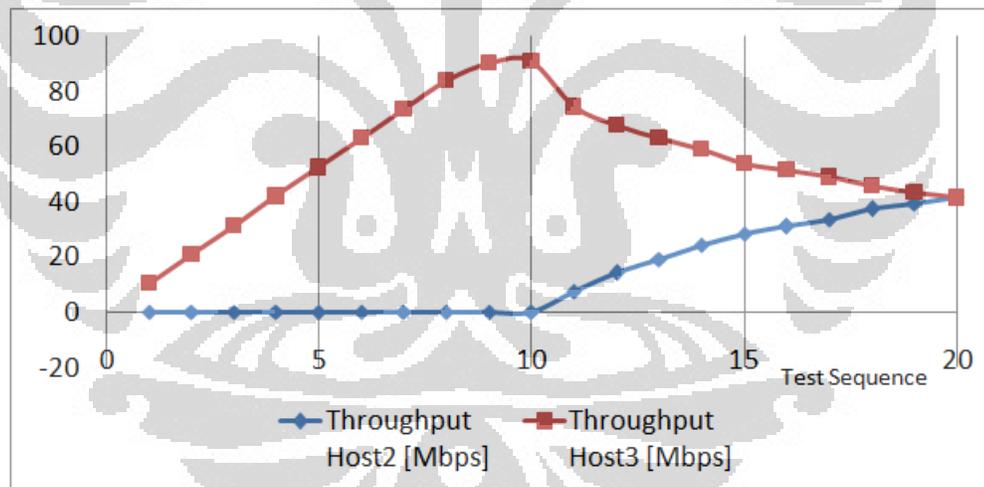
Gambar 4.2. Metode Pengujian Throughput

#### 4.1.1. Metode Pengujian *Throughput*

Pada Gambar 4.2. menunjukkan metode pengujian *throughput*, pengujian dilakukan sebanyak 20 kali dengan mengirimkan *traffic* ke dua *Node Client* yang berbeda, *Host2* dan *Host3*. Pada setiap kali pengujian, transmisi *traffic* ke *Host3* dinaikan 10 Mbps, sampai dengan kecepatan maksimum 100 Mbps, yang merupakan alokasi maksimum kanal utama yang disediakan untuk pengujian. Pada setiap pengujian selanjutnya, pengiriman trafik ke *Host2* dinaikan 10 Mbps, hingga mencapai kecepatan maksimum 100 Mbps.

Pengukuran dilakukan untuk membuktikan maksimum *throughput* yang bisa dicapai pada kedua *Host*. Pada 20 pengujian pertama, kedua *host* tidak melakukan registrasi ke CSCF, dan pada 20 pengujian berikutnya, *Host2* melakukan registrasi ke CSCF.

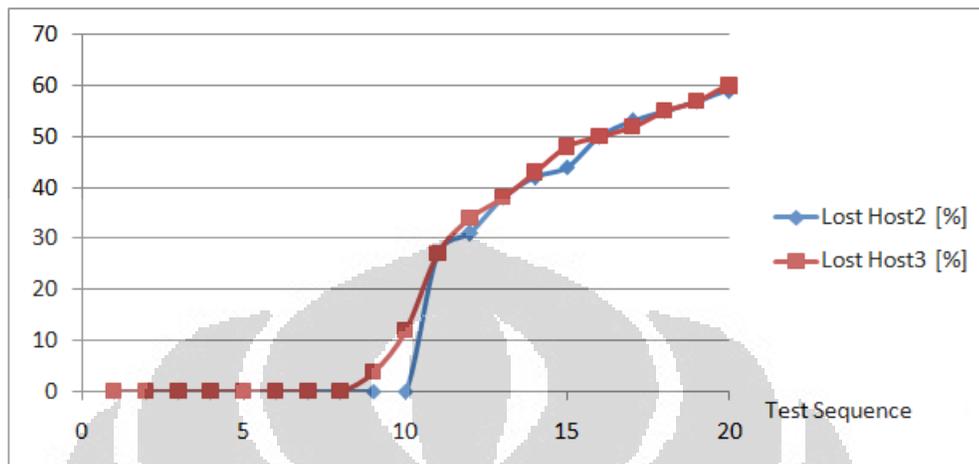
#### 4.1.2. Hasil Pengujian *Throughput*



Gambar 4.3. Throughput dan Jitter unregistered UE

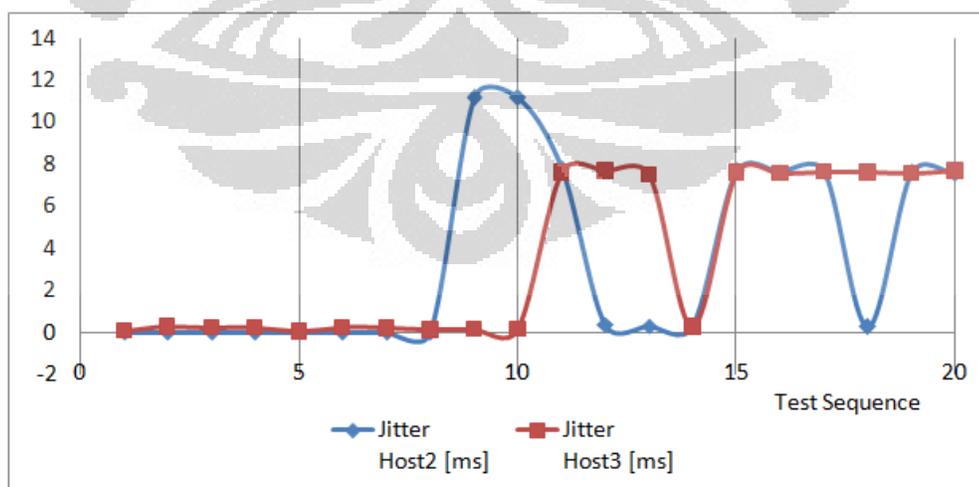
Hasil pengujian pada kondisi *Host2* dan *Host3* tidak melakukan registrasi ke CSCF menunjukkan bahwa kecepatan transmisi data menuju kedua *host* tersebut memiliki kemungkinan yang sama. Hingga pengujian kesembilan, *Host3* dilayani dengan sesuai dengan kecepatan transmisi yang dikirimkan dan mengalami saturasi pada kecepatan 90 Mbps (Gambar 4.3), ditandai dengan adanya *loss packet* sebesar 3.8%. Pada pengujian kesepuluh tidak terjadi peningkatan

kecepatan yang signifikan pada pengiriman transmisi menuju *Host3*, namun *packet loss* meningkat menjadi 12% (Gambar 4.4).



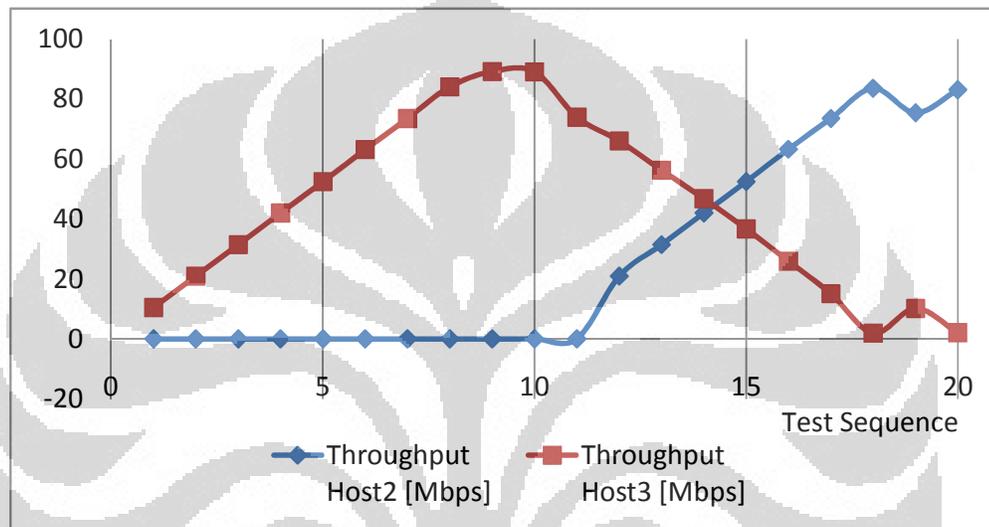
Gambar 4.4. % Packet Loss pada unregistered UE

Pada pengujian kesebelas kecepatan pengiriman transmisi menuju *Host2* mulai dinaikan 10 Mbps dan pengiriman transmisi menuju *Host3* dibuat tetap pada 100 Mbps, dari Gambar 4.3 terlihat setiap kenaikan kecepatan penerimaan transmisi pada *Host2* mengakibatkan penurunan kecepatan penerimaan transmisi pada *Host3*, dengan percepatan yang hampir sama. Pada pengujian kedua puluh dan dua puluh satu kecepatan transmisi menuju *Host2* dan *Host3* pada posisi 100 Mbps, kecepatan penerimaan pada kedua *Host* memiliki nilai pada kisaran 42 Mbps dan *jitter* pada kisaran 7.5 ms (Gambar 4.5).



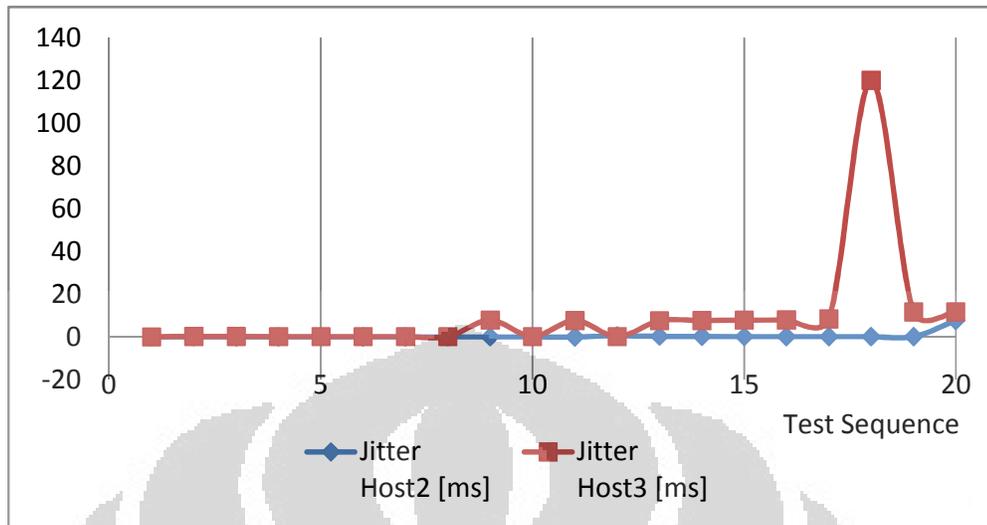
Gambar 4.5. Jitter pada unregistered UE

Kondisi *Throughput* dan *Packet Loss* yang seimbang pada *Traffic* menuju *host2* dan *host3* ini dikarenakan kedua *node* tersebut memiliki prioritas yang sama, sehingga PDP akan melakukan mekanisme *queuing* yang seimbang dan mengakibatkan kedua *node* memiliki variasi keterlambatan (*Jitter*) yang sama (Gambar 4.5.)



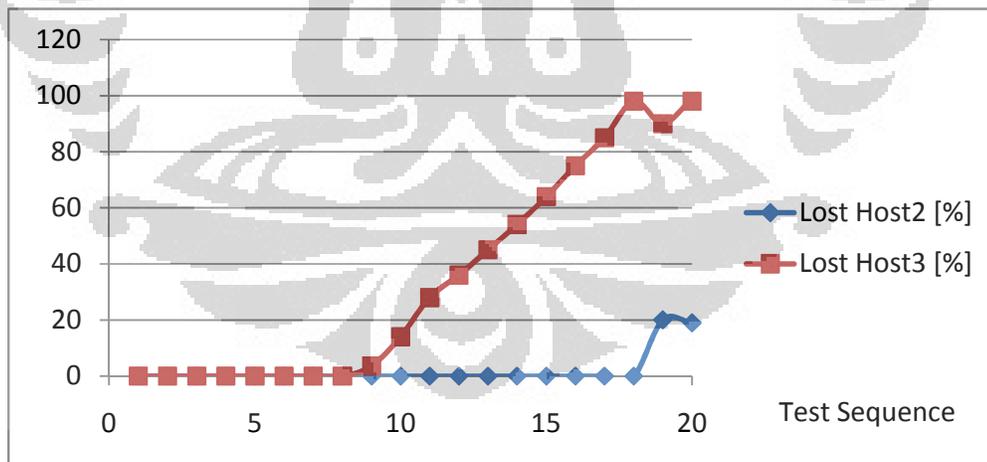
Gambar 4.6. *Throughput* pada *registered UE*

Hasil pengujian pada kondisi *Host2* melakukan registrasi ke CSCF menunjukkan bahwa kecepatan transmisi data menuju *Host2* tersebut memiliki prioritas yang lebih tinggi dibanding transmisi menuju *Host3*. Hingga pengujian kesembilan, *Host3* dilayani dengan sesuai dengan kecepatan transmisi yang dikirimkan dan mengalami saturasi pada kecepatan 89 Mbps (Gambar 4.6), ditandai dengan adanya *packet loss* sebesar 3.6%. Pada pengujian kesepuluh tidak terjadi peningkatan kecepatan yang signifikan pada pengiriman transmisi menuju *Host3*, namun *packet loss* meningkat menjadi 14% (Gambar 4.8).



Gambar 4.7. *Jitter* pada *registered UE*

Pada pengujian kesebelas kecepatan pengiriman transmisi menuju *Host2* mulai dinaikan 10 Mbps dan pengiriman transmisi menuju *Host3* dibuat tetap pada 100 Mbps, dari Gambar 4.6 terlihat setiap kenaikan kecepatan penerimaan transmisi pada *Host2* mengakibatkan penurunan kecepatan penerimaan transmisi pada *Host3*, dengan percepatan yang hampir sama.



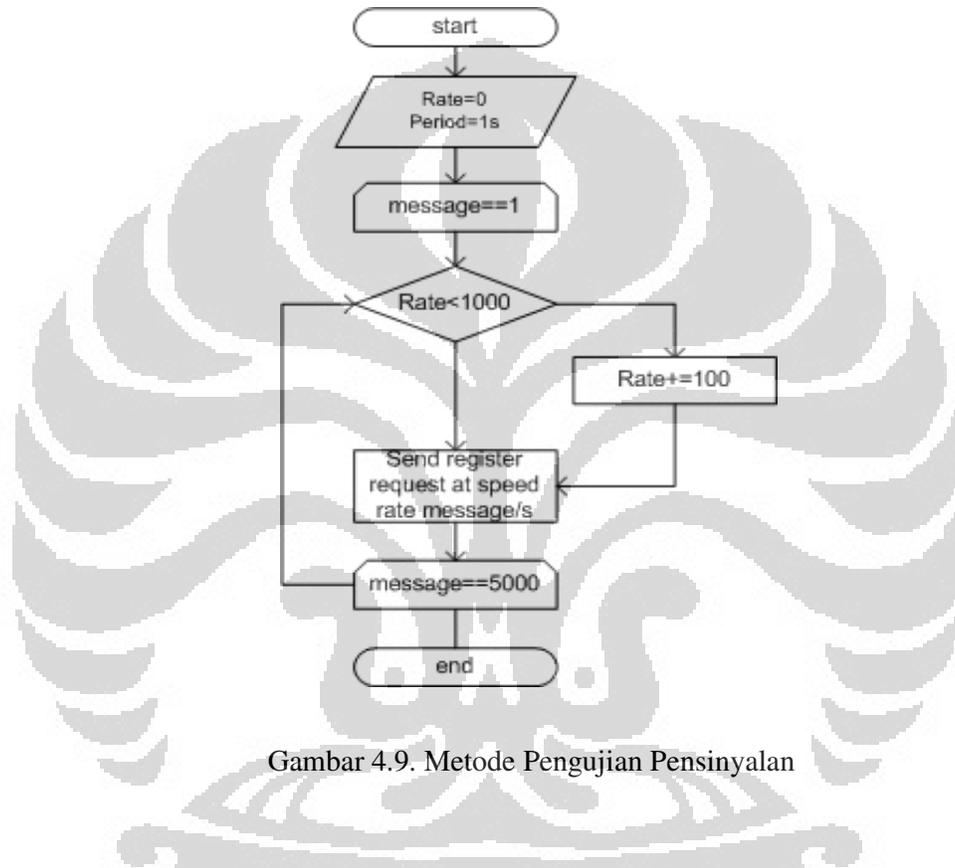
Gambar 4.8. *% Packet Loss* pada *registered UE*

Kecepatan pengiriman *traffic* menuju *Host2* selalu dilayani dan tidak mengalami *packet loss* hingga pengujian ke 18, pada titik ini kecepatan penerimaan di sisi *Host2* mencapai 84 Mbps dan tidak memberikan ruang bagi trafik menuju *Host3*.

Hal ini ditunjukkan dengan kecepatan penerimaan pada *Host3* mencapai titik terendah 1.96 Mbps dan *Jitter* tertinggi 120 ms (Gambar 4.7)..

#### 4.2. Pengaruh pada Pensinyalan

Pengaruh penerapan QoS terhadap pensinyalan diuji sebagai berikut.



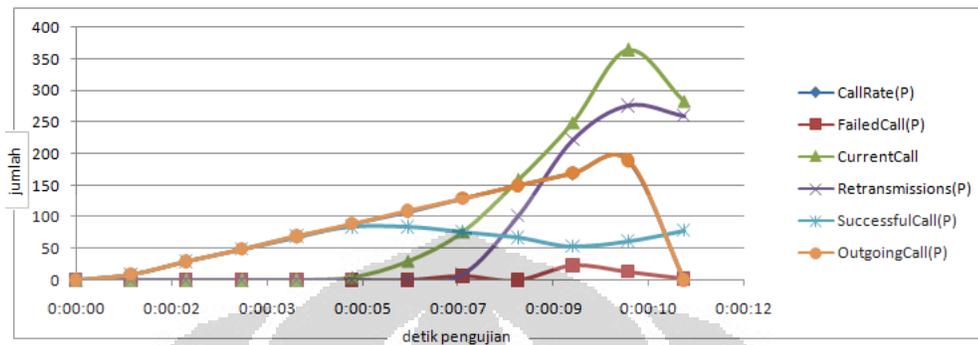
Gambar 4.9. Metode Pengujian Pensinyalan

##### 4.2.1. Metode Pengujian Signalling

Pada pengujian ini dibandingkan kinerja SIP signalling untuk tiga skenario implementasi yang berbeda. Metode pengujian digambarkan pada Gambar 4.9

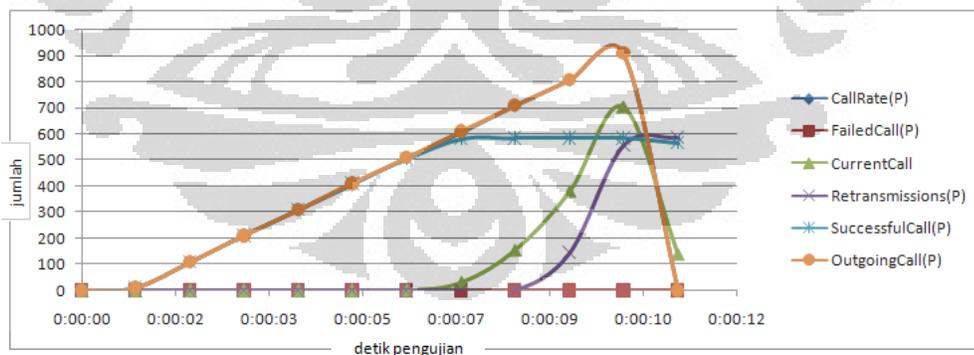
Kondisi pertama adalah penerapan dengan CSCF, PDP, dan PEP pada mesin yang berbeda. Komunikasi diantara ketiga komponen dilakukan dengan menggunakan *Web Service*. Pengujian untuk mengukur pengaruh penerapan QoS terhadap kinerja SIP signalling dilakukan dengan mengirimkan pesan registrasi dengan *Call Rate* yang naik 20 call/sec setiap periode 1 detik, dari 0 hingga maksimum

*Call Rate* 200 call/sec, dan berhenti jika jumlah pengiriman mencapai 5000 pesan. Hasil pengujian ditampilkan pada Gambar 4.10.



Gambar 4.10. Kinerja SIP dengan pemisahan CSCF, PDP dan PEP

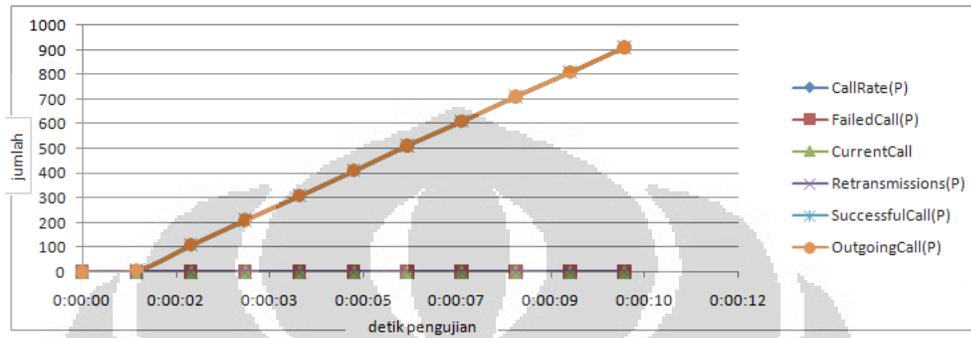
Kondisi kedua adalah penerapan dengan CSCF dan PDP pada mesin yang sama, PEP pada mesin yang berbeda. Komunikasi diantara PDP dan PEP dilakukan dengan menggunakan *Web Service*. Pengujian untuk mengukur pengaruh penerapan *QoS* terhadap kinerja SIP signalling dilakukan dengan mengirimkan pesan registrasi dengan *Call Rate* yang naik 100 call/sec setiap periode 1 detik, dari 0 hingga maksimum *Call Rate* 1000 call/sec. Pengujian dilakukan hingga jumlah pesan yang dikirimkan mencapai 5000 pesan registrasi. Hasil pengujian ditampilkan pada Gambar 4.11.



Gambar 4.11. Kinerja SIP dengan CSCF dan PDP pada mesin yang sama

Kondisi ketiga adalah implementasi dengan CSCF dan PDP pada mesin yang sama, PEP pada mesin yang berbeda. Output dari proses pada CSCF langsung disimpan kedalam database, dan tidak menunggu *Return Code* dari proses PDP.

PDP selalu melihat perubahan yang terjadi pada database, jika ada status registrasi baru, maka PDP akan melakukan fungsi lebih lanjut dalam penerapan *Policy*. Komunikasi diantara PDP dan PEP dilakukan dengan menggunakan *Web Service*.



Gambar 4.12. Kinerja SIP CSCF independen terhadap PDP

Pengujian untuk mengukur pengaruh penerapan QoS terhadap kinerja pensinyalan SIP dilakukan dengan mengirimkan pesan registrasi dengan *Call Rate* yang naik 100 call/sec setiap periode 1 detik, dari 0 hingga maksimum *Call Rate* 1000 call/sec. Pengujian dilakukan hingga jumlah pesan yang dikirimkan mencapai 5000 pesan registrasi. Hasil pengujian ditampilkan pada Gambar 4.12.

#### 4.1.2. Hasil Pengujian Signalling

Penerapan dengan menggunakan solusi berbasis *Web Service* pada arsitektur yang dibangun berpengaruh pada turunnya kinerja pensinyalan berbasis SIP dalam melayani registrasi terminal hingga kurang dari 100 call/sec ( garis dengan tanda asterik). Pada saat *Outgoing Call* mendekati 100, jumlah panggilan yang belum diselesaikan (*Current Call*) dalam masa 1 detik mulai meningkat ( garis dengan tanda segi tiga). Pada detik ke tujuh permintaan yang belum selesai dan sudah melewati masa timeout mengalami kegagalan. *Retransmisi* ( garis dengan tanda silang ) meningkat seiring dengan semakin banyaknya permintaan yang mengalami *timeout* dikarenakan keterlambatan respon dari *server* CSCF. Penurunan kinerja pada skenario ini disebabkan CSCF menunggu respon balik

dari PDP, dan PDP menunggu respon balik dari PEP pada pemrosesan setiap permintaan penerapan *Policy*.

Pada hasil pengujian penempatan CSCF dan PDP pada mesin yang sama, dan menggunakan komunikasi berbasis *Web Service* hanya untuk komunikasi antara PDP dan PEP menunjukkan peningkatan kinerja hingga mendekati 600 call/sec. Hingga pengiriman 1000 call/sec dan total 5000 pesan yang dikirimkan tidak terjadi kegagalan panggilan, hanya saja terjadi keterlambatan pelayanan oleh CSCF yang ditandai dengan naiknya antrian permintaan yang belum selesai di proses.

Pada pengujian skenario CSCF yang independen terhadap proses analisa *Policy* pada PDP, didapatkan hasil pengukuran yang lebih baik dari skenario sebelumnya. Tidak terjadi antrian Call hingga pengukuran mencapai 1000 call/sec. Model arsitektur ini mendekati kondisi alamiah dari sebuah CSCF, namun keterlambatan penerapan *Policy* tetap ditemukan pada sistem ini dan terdeteksi dengan kondisi masih terjadinya pemrosesan permintaan di sisi PEP pada saat CSCF sudah lama menyelesaikan 5000 pesan registrasi.

## BAB 5

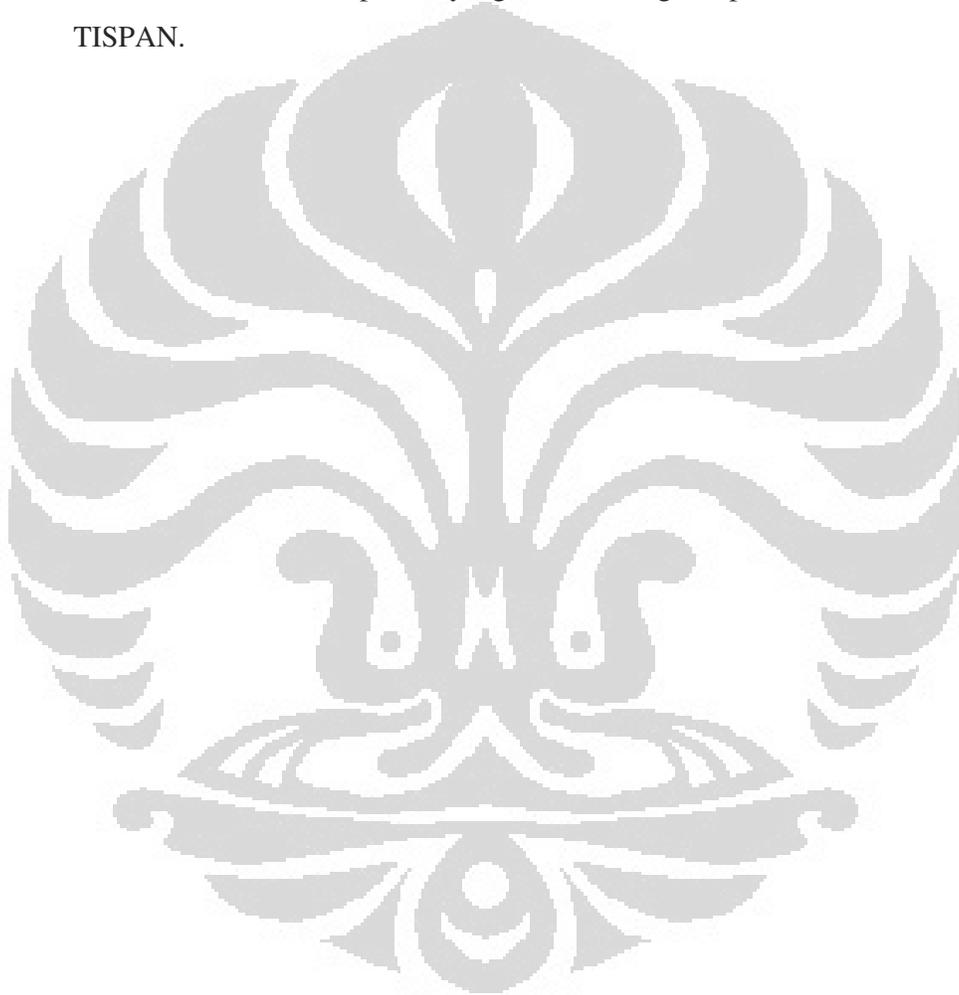
### KESIMPULAN

Pada tulisan ini telah diuraikan penerapan QoS dan kontrol pengaksesan jaringan berbasis protokol SIP. Pemodelan arsitektur mengacu pada definisi IETF mengenai *Policy Based Admission Control*, dan menggunakan sebagian komponen-komponen dan fungsi arsitektur NGN IMS dari ETSI TISPAN, serta konsep penerapan QoS pada subsistem RACS. Penerapan pada arsitektur yang dibangun tidak menggunakan spesifikasi yang didefinisikan oleh standar RACS dalam hal komunikasi antar komponen, namun menggunakan solusi berbasis *Web Service*.

Dari rancang bangun dan pengujian didapatkan hasil sebagai berikut:

1. Penerapan kebijakan jaringan dapat dilakukan dengan memanfaatkan status dari sesi registrasi maupun *Call Setup* dan *Call Teardown* protokol SIP.
2. Telah dilakukan modifikasi komponen CSCF, dan membangun komponen *Policy Decision Point* (PDP), dan *Policy Enforcement Point* (PEP)
3. *Web Service* bisa digunakan untuk komunikasi antar komponen CSCF, PDP dan PEP dalam pemrosesan pesan protokol SIP, analisa penerapan kebijakan jaringan dan penerapan aturan kebijakan dan pengontrolan pengaksesan jaringan.
4. Penambahan fungsi komunikasi pada CSCF berpengaruh pada penurunan kinerja pelayanan pemrosesan *Call Control*.
5. Penurunan kinerja pada fungsi *Call Control* hingga mendekati 100 call/sec pada skenario pemisahan penuh antara CSCF, PDP dan PEP, dan 600 call/sec pada skenario penggabungan CSCF dan PDP.

6. Skenario tanpa umpan balik antara CSCF dan PDP menunjukkan kondisi kinerja yang lebih baik, pada skenario ini CSCF dapat memproses pesan registrasi SIP tanpa ada antrian hingga batas pengujian 1000 call/sec dengan total 5000 pesan registrasi.
7. Pengembangan lebih lanjut perlu dilakukan untuk mengurangi penurunan performansi pada layanan *Call Control* berbasis SIP dan penerapan protokol komunikasi antar komponen yang sesuai dengan spesifikasi RACS ETSI TISPAN.



## DAFTAR ACUAN

- [1] OAA100101, Huawei, NGN System Overview, Huawei Technologies Co., Ltd., 2006
- [2] OAA10000206, Huawei, NGN Protocol Overview, Huawei Technologies Co., Ltd., 2006
- [3] OAA10000706, Huawei, SIP, Huawei Technologies Co., Ltd., 2006
- [4] Handley M., Schulzrinne H., Schooler E., Rosenberg J., ACIRI, Columbia U, Cal Tech, Bell Labs, 1999
- [5] CNAP, CCNP, Multiyaer Switching v3.0, Cisco, 2003.
- [6] Mirzaie S., Preventing of SYN Flood attack with iptables Firewall, Second International Conference on Communication Software and Networks, 2010
- [7] Balan D.G, Potorac D.A., Linux HTB Queuing Discipline Implementations, Networked Digital Technologies, 2009
- [8] Simon E., Gressier E., Berthelin J., Avoid LAN Switches-IP Routers provide a better alternative for a Real-Time Communication System, 2nd Intl. Workshop on Real-Time LANs in the Internet Age, 2003
- [9] Lei J., Hogrefe D., IP Multimedia Subsystem (IMS), Telematics group University of Goettingen, 2008, <http://www.3g4g.co.uk/Ims/IMS.pdf>, Last Accessed: December 17, 2010.
- [10] Magedanz T., Open EPC – A Short Overview, Fraunhofer FOKUS, 2010, [http://www.openepc.net/en/openepc/\\_docs/OpenEPC\\_tutorial.pdf](http://www.openepc.net/en/openepc/_docs/OpenEPC_tutorial.pdf), Last Accessed: December 17, 2010.
- [11] Rutgers., Linux Security , State University of New Jersey, 2010, <http://coewww.rutgers.edu/www1/linuxclass2003/lessons/lecture9.html>, Last Accessed: December 17, 2010.
- [12] Marsh M.G., Policy Routing Book, Paktronix Systems, LLC. ,2001,<http://www.policyrouting.org/iproute2.doc.html>, Last Accessed: December 17, 2010.

- [13] Jasmina B., Priority Transmission of SIP Signaling Flows over IP Network, Cabinet of CEO BH Telecom, Joint Stock Company, Sarajevo Sarajevo, Bosnia and Herzegovina, 2009
- [14] Mehdi S., A Proposed Model for QoS Provisioning in IMS-based IPTV Subsystem, Communication Technology Institute Iran Telecommunication Research Center Tehran, Iran, 2009
- [15] Li Zhao, Analysis of A Scheme Supporting End-to-End QoS for VoIP Emergency Calls, Guilin University of Electronic Technology, Guilin 541004, China, 2008
- [16] Hassan Y., NGN Functional Architecture for Resource Allocation and Admission Control, NIS, TELSİK, Serbia, 2009
- [17] Cho IL., A Centralized Resource and Admission Control Scheme for NGN Core Network, Graduate School of Information Science and Electrical Engineering, Kyushu University 6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan, 2009
- [18] Koji T., A Modeling Method of Access Network for Resource Reservation and Admission Control of NGN, NTT Network Service Systems Laboratories -9-11, Midori-Cho Musashino-Shi, Tokyo 180-8585 Japan, 2010
- [19] Jing S., Flow Management with Service Differentiation for SIP Application Server, The Third ChinaGrid Annual Conference, 2005
- [20] Garcia R.M., Design and Development of a CNG oriented to Embedded Linux, Universitat Politecnica De Catalunya, Spain, 2010
- [21] Egger C., Happenhofer M., Fabini J., Reichl P., BIQINI – A Flow-based QoS Enforcement Architecture for NGN Services, Vienna University of Technology Institute of Broadband Communications, Telecommunications Research Center Vienna (FTW), Austria, 2010
- [22] Karandikar A., Broadband Networks: Concepts and Technology, IIT Bombay, India, <http://nptel.iitm.ac.in/video.php?subjectId=117101050>, Last Accessed: July 6, 2012