

# ANALISIS PENERAPAN DIFFSERV PADA TEKNOLOGI TCP/IP TRADISIONAL UNTUK JARINGAN PERANGKAT TELEKOMUNIKASI 3G BERBASIS IP DI PT INDOSAT, TBK. CABANG MALANG

**Okma Winarko Putro**

Program Studi Teknik Informatika  
STMIK PPKIA Pradnya Paramita  
Jl. Laksda Adi Sucipto 249-A Malang  
E-mail: okma.putro@gmail.com

## ABSTRACT

*The third generation mobile communication technology or 3G allows users to enjoy various high-speed communications services. PT Indosat, Tbk. as one of the leading mobile operators in Indonesia builds IP-based 3G telecommunications network in Malang, which consists of 3G cellular network transmitters (Node B) and Radio Network Controller (RNC), over an IP/MPLS network that become the communication line among 3G telecommunication network elements. Network devices with traditional TCP/IP concept, which is the beginning of IP/MPLS development, has a lower implementation cost and a feature to implement DiffServ (Differentiated Services) to improve Quality of Service (QoS). The goal of this research is to design and build a small-scale traditional TCP/IP network (testbed) and performing analysis on the Diffserv implementation. The analysis shows that DiffServ can be applied to the designed network and able to improve QoS by making priorities based on Differentiated Service Code Point (DSCP). The testbed network is also capable of handling 3 Node B which is connected to 1 RNC.*

**Key words:** *Diffserv, QoS, TCP/IP, 3G.*

## PENDAHULUAN

Perkembangan teknologi komunikasi seluler / *mobile communication* di Indonesia saat ini telah berada pada generasi ketiga atau lebih dikenal dengan istilah *Third Generation* (3G). Dengan adanya teknologi ini, pelanggan telekomunikasi seluler dapat menikmati layanan-layanan *broadband* yang disediakan oleh operator terutama layanan paket data Internet berkecepatan tinggi. Kemampuan perangkat telekomunikasi 3G dalam menyediakan layanan *broadband* juga harus diimbangi dengan kapabilitas jaringan yang menghubungkan antar-perangkat tersebut. Sampai saat ini, jaringan TCP/IP masih merupakan pondasi bagi sebagian besar jaringan komputer di dunia, termasuk dalam

memenuhi kebutuhan pada perangkat telekomunikasi.

PT Indosat, Tbk. merupakan salah satu operator penyedia layanan telekomunikasi seluler yang terkemuka di Indonesia telah mengimplementasikan lebih dari 30 pemancar layanan seluler 3G (Node B) yang tersebar di area Kota Malang. Seluruh Node B tersebut terhubung dengan sebuah Radio Network Controller (RNC) yang berada di kantor cabang Malang melalui jaringan TCP/IP yang digabungkan dengan teknologi IP/MPLS. Implementasi dari teknologi IP/MPLS ini tentu saja menelan biaya yang tidak sedikit, sedangkan perangkat jaringan dengan teknologi TCP/IP tradisional yang merupakan pondasi awal dari pengembangan menuju

teknologi IP/MPLS tersebut masih bisa digunakan dalam menangani jaringan perangkat telekomunikasi 3G berbasis IP. *Diffserv* merupakan salah satu metode dalam menjaga QoS pada jaringan TCP/IP dengan cara memberi tanda pada setiap paket data dan memberikan prioritas berdasarkan tanda tersebut. Tanda ini dinamakan *Differentiated Service Code Point* (DSCP) yang terletak pada *header* paket IP menggantikan *field Type of Service* (ToS) pada jenis perangkat *router* lama, sehingga implementasi dari metode ini tidak memerlukan protokol tambahan.

Dengan menerapkan metode *diffserv* (*Differentiated Service*) pada sebuah perangkat jaringan TCP/IP tradisional, perangkat tersebut mampu memberikan perbaikan *Quality of Service* (QoS) dengan cara memberikan prioritas dan perlakuan berbeda pada paket data sesuai dengan karakteristik *traffic* data yang saling dikirimkan pada sebuah jaringan perangkat telekomunikasi 3G berbasis IP. Selain itu, sebagian besar perangkat TCP/IP tradisional telah mampu mendukung implementasi dari metode *diffserv* ini.

### **Rumusan Masalah**

Berdasarkan latar belakang yang telah dipaparkan, maka masalah dalam penelitian ini adalah bagaimana melakukan pengujian dan analisis terhadap penerapan *diffserv* pada teknologi TCP/IP tradisional untuk Jaringan Perangkat Telekomunikasi 3G Berbasis IP di PT Indosat, Tbk. Cabang Malang.

### **Tujuan Penelitian**

Tujuan dari penelitian ini adalah untuk melakukan pengujian dan analisis dari penerapan metode *diffserv* pada jaringan TCP/IP tradisional sehingga mampu memberikan perbaikan *Quality of Service* (QoS) dalam menangani perangkat telekomunikasi 3G berbasis IP yang saling terintegrasi melalui jaringan tersebut.

## **LANDASAN TEORI**

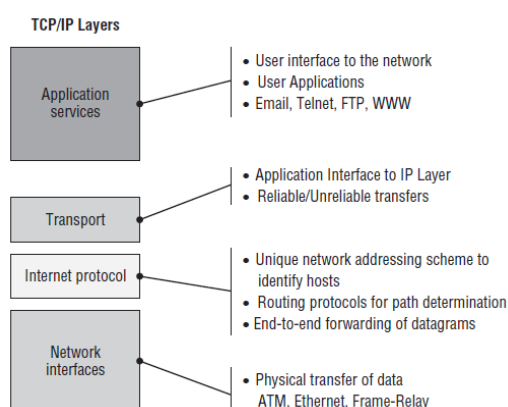
### **Teknologi Komunikasi Seluler**

Teknologi komunikasi seluler merupakan teknologi komunikasi nirkabel (*wireless*) dimana area jangkauan yang dilayani dibagi menjadi beberapa *cell* (sel) atau bagian-bagian kecil (William, C.Y Lee, 2006:85). Sebuah *cell* terdiri dari satu atau lebih *transmitter* (pemancar) dan luas jangkauannya tergantung pada besarnya daya pancar *transmitter* tersebut. Konsep dasar dari sistem seluler adalah penggunaan pemancar daya rendah untuk memungkinkan penggunaan kembali dan efisiensi dari frekuensi. Teknologi komunikasi seluler merupakan teknologi komunikasi nirkabel (*wireless*) dimana area jangkauan yang dilayani dibagi menjadi beberapa *cell* (sel) atau bagian-bagian kecil (William, C.Y Lee, 2006:85). Sebuah *cell* terdiri dari satu atau lebih *transmitter* (pemancar) dan luas jangkauannya tergantung pada besarnya daya pancar *transmitter* tersebut. Konsep dasar dari sistem seluler adalah penggunaan pemancar daya rendah untuk memungkinkan penggunaan kembali dan efisiensi dari frekuensi. Teknologi komunikasi *mobile* / seluler memiliki arsitektur jaringan yang melibatkan banyak *Network*

*Element* (NE) yang dibagi kedalam 2 bagian besar yaitu *Access Network* (AN) dan *Core Network* (CN). Perangkat telekomunikasi pada setiap bagian besar saling berinteraksi menggunakan sistem pensinyalan (*signalling system*) yang dilewatkan melalui *Internet Protocol* (IP).

### Model TCP/IP Layer

Model TCP/IP (Transmission Control Protocol /Internet Protocol) pada awalnya dikembangkan oleh ARPA (Advanced Research Project Agency) dari Departemen Pertahanan Amerika Serikat pada tahun 1969. TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat *independent* terhadap mekanisme *transport* jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP address*) yang memungkinkan beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lain di internet. Protokol TCP / IP dirancang kedalam empat lapisan teknologi, seperti yang digambarkan pada gambar 1.



**Gambar 1** Pemodelan *Layer* TCP/IP

*Application layer* adalah lapisan yang berhadapan langsung dengan pengguna / *user* yang berfungsi untuk menangani *high-level protocol*, masalah representasi data, proses *encoding* dan *dialog control* yang memungkinkan terjadinya komunikasi antar aplikasi jaringan. *Layer* ini berisi spesifikasi protokol-protokol khusus yang menangani aplikasi umum seperti *Telnet*, *File Transfer Protocol* (FTP), *Domain Name System* (DNS), dan lain-lain.

*Transport layer* menyediakan layanan pengiriman dari sumber data menuju ke tujuan dengan cara membuat *logical connection* antara keduanya. *Layer* ini bertugas untuk memecah data dan membangun kembali data yang diterima dari *application layer* ke dalam aliran data yang sama antara sumber dan pengirim data. *Transport layer* juga menangani masalah *reliability*, *flow control* dan *error correction*. *Layer* ini terdiri dari dua protokol yaitu TCP dan UDP.

*Internet Protocol Layer* memiliki tugas utama untuk memilih jalur terbaik yang akan dilewati oleh paket data dalam sebuah jaringan. Selain itu, *layer* ini juga bertugas melakukan *packet switching* untuk mendukung tugas utama tersebut. *Layer* ini terdiri dari *Internet Protocol* (IP), *Internet Control Message Protocol* (ICMP), *Address Resolution Protocol* (ARP), dan *Reverse Address Resolution Protocol* (RARP).

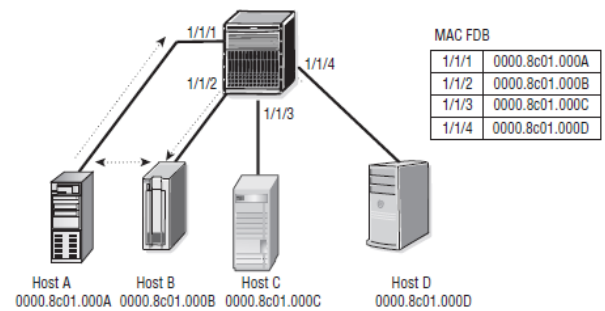
*Network interface layer* adalah lapisan paling bawah dari model TCP ini yang berfungsi sebagai *device driver* yang memungkinkan *datagram* IP dikirim ke atau dari *physical network*. Jaringan dapat berupa sebuah kabel,

*Ethernet, frame relay, Token ring, ISDN, ATM* , jaringan radio, satelit atau alat lain yang dapat mentransfer data dari sistem ke sistem.

### Perangkat Jaringan Switch dan Router

Dalam membentuk jaringan komputer lokal (LAN) yang menghubungkan lebih dari dua komputer, diperlukan adanya perangkat pemusat (*concentrator*) komputer yang terhubung melalui media fisik berupa kabel dan konektor. Perangkat yang digunakan dalam menghubungkan komputer-komputer ini adalah *switch*. Sebuah *ethernet switch* mampu menghubungkan beberapa *host* dengan metode komunikasi *full-duplex*, yaitu seluruh *host* dapat berkomunikasi secara simultan. *Switch* bekerja pada layer 2 OSI dengan menggunakan *intelligent switching*, yaitu mempelajari *MAC address* (Medium Access Control) dari setiap *host* yang terhubung. Data port dan *MAC address* dari setiap *host* kemudian disimpan dalam sebuah *forwarding database* (FDB). Pada saat *host* mengirimkan data, *switch* memeriksa *header* dari *frame* data yang dikirim untuk dicocokkan dengan *host* yang memiliki *MAC address* tujuan, dan dengan cara ini data secara langsung dikirimkan ke *host* tujuan tanpa melibatkan *host* lain seperti yang dilakukan pada penggunaan *hub*. Pada Gambar 2 terlihat apabila *Host A* akan melakukan pengiriman data kepada *Host B*, maka *switch* hanya akan meneruskan *frame* data ke *Host B* dengan mencocokkan *MAC address* tujuan yang dibaca dengan *forwarding database* yang telah dibangun

sebelumnya.



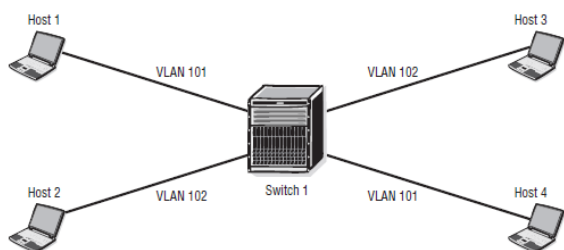
**Gambar 2 Prinsip Kerja Switch**

*Router* adalah perangkat jaringan yang berfungsi meneruskan paket data dari suatu jaringan (*network*) menuju jaringan lain. Perangkat jaringan ini bekerja pada *layer 3* OSI dan saling berkomunikasi dengan menggunakan protokol *routing*

### Virtual Lan (VLAN)

*Virtual LAN* (VLAN) adalah sebuah mekanisme yang memungkinkan pengguna untuk membentuk jaringan pada suatu lokasi secara virtual tanpa bergantung pada lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana bisa dilakukan pembentukan segmen jaringan yang berdasarkan kategori, organisasi atau departemen tanpa bergantung pada lokasi *host*. VLAN dibentuk melalui *switch* yang mendukung fasilitas *VLAN tagging* (*manage-able switch*) dan menggunakan VID (VLAN ID) berupa angka antara 1 – 4094 sebagai penanda keanggotaan jaringan. *VLAN assignment* atau pemberian keanggotaan VLAN kepada *host* secara umum dilakukan dengan metode *port-based* yaitu sesuai dengan nomor *interface* tempat tersambungannya *host* pada *switch*. VLAN 1

adalah default VLAN, yang berarti sebelum dilakukan segmentasi VLAN, seluruh *host* yang terhubung dalam *switch* tersebut menggunakan jalur VLAN 1 untuk berkomunikasi. Segmentasi jaringan dilakukan ketika seorang administrator jaringan membuat VLAN baru dan menugaskannya pada port tertentu tempat *host* terhubung. *Host* hanya akan bisa berkomunikasi dengan *host* lain dengan VLAN yang sama. Sebagai contoh pada Gambar 3 menggunakan VLAN 101 dan 102, maka *Host* 1 hanya bisa melakukan komunikasi dengan *Host* 4. Komunikasi data antar VLAN tidak bisa dilakukan kecuali melewati sebuah *router* yang telah diberi konfigurasi untuk melakukan *routing* antar VLAN.



**Gambar 3** Penugasan VLAN pada *switch*

Ekspansi jaringan dalam konfigurasi VLAN ini tidak terbatas dalam satu perangkat *switch* saja, namun *host* dengan yang tergabung dalam VLAN yang sama mampu melakukan komunikasi data melalui *switch* lain dengan cara melakukan *VLAN trunking* (802.1Q). *VLAN Trunking* dilakukan dengan mengkonfigurasi sebuah *interface* terpisah yang dijadikan sebagai penghubung antara 2 *switch*, kemudian mengizinkan VLAN yang akan dilewatkan melalui *interface* tersebut.

Dengan ini, maka kedua *switch* mampu melakukan pertukaran *forwarding database* (FDB) dan menghubungkan *host* dengan VLAN ID yang sama pada *switch* yang terpisah.

### **Quality of Service (QoS) Pada Jaringan IP**

*Quality of Service* atau umumnya disingkat *QoS* merupakan kemampuan untuk menyediakan jaminan performansi dalam berbagai keadaan beban jaringan. Dalam *QoS*, parameter yang menjadi tolak ukur kehandalan sebuah jaringan adalah *throughput*, *delay/latency*, *jitter*, *packet loss*, dan *utilization*.

#### 1. *Throughput*

*Throughput* adalah ukuran rata-rata dari jumlah data yang dapat dikirim melewati jaringan dan dispesifikasikan dalam bit per second (bps). Dalam pengukuran *throughput* jaringan dengan kapasitas lebih besar umumnya menggunakan satuan *megabit per second* (Mbps) dan *gigabit per second* (Gbps).

#### 2. *Delay/Latency*

*Delay* atau *latency* adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya.

#### 3. *Jitter*

*Jitter* merupakan variasi *delay* antar paket yang terjadi pada jaringan *packet-switched*. Besarnya nilai *jitter* akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (*congestion*). Semakin besar beban trafik di dalam jaringan akan menyebabkan

semakin besar pula peluang terjadinya *congestion* dengan demikian nilai *jitter*-nya akan semakin besar. Semakin besar nilai *jitter* akan mengakibatkan nilai *QoS* akan semakin turun.

#### 4. *Packet Loss*

*Packet loss* didefinisikan sebagai kegagalan transmisi paket IP dalam mencapai tujuannya. Kegagalan tersebut disebabkan oleh beberapa faktor yaitu :

- a. Terjadinya *congestion* akibat *traffic overload* dalam jaringan tersebut.
- b. *Error* yang terjadi pada media fisik (kabel, *connector* dan perangkat transmisi).
- c. Kegagalan yang terjadi pada sisi penerima yang bisa disebabkan karena *overflow* yang terjadi pada *buffer*.

#### **Metode *Integrated Service (Intserv)* dan *Differentiated Service (Diffserv)***

Metode penerapan *QoS* dalam sebuah jaringan IP sangat bervariasi dan menyesuaikan dengan kebutuhan *client*. Secara default, sebuah jaringan menerapkan *best-effort service* yang berarti semua paket IP diperlakukan dengan sama dan sebuah jaringan hanya memastikan paket tersebut sampai kepada tujuan tanpa mempertimbangkan sensitifitas terhadap *delay*, fluktuasi *bandwidth*, dan perubahan kondisi jaringan. Metode *best-effort* tidak dapat diaplikasikan untuk layanan *voice* dan layanan lain yang membutuhkan keadaan dimana *delay* dan *jitter* harus dalam kondisi rendah. Dengan banyaknya penggunaan jaringan IP untuk melewati suara, video

---

Jurnal Teknologi Informasi Vol. 4 No. 2

dan beberapa kebutuhan aplikasi perangkat telekomunikasi, maka arsitektur *QoS* merupakan pondasi utama dalam menjaga kelancaran komunikasi. Arsitektur *QoS* dibagi menjadi 2 yaitu arsitektur *Integrated Service* dan arsitektur *Differentiated Service*.

Arsitektur *Integrated Service (Intserv)* menyediakan *QoS* untuk paket IP dengan mengirimkan sinyal ke jaringan bahwa mereka memerlukan *QoS* dalam pengiriman paket untuk kemudian melakukan pemesanan *bandwidth* untuk sebuah aplikasi. *Integrated Service* tidak dirancang untuk jaringan berskala besar, sehingga hanya cocok bagi jaringan berukuran kecil dan menengah. Sistem pemesanan sumber daya (*bandwidth*) memerlukan protokol tersendiri. Salah satu protokol yang sering digunakan adalah *Resource Reservation Protocol (RSVP)*.

Arsitektur *Differentiated Service (Diffserv)* memiliki skema implementasi *QoS* dengan membagi trafik jaringan kedalam beberapa kelas dan memperlakukan setiap kelas secara berbeda. Identifikasi kelas dilakukan dengan memasang kode yang disebut *Differentiated Service Code Point (DSCP)* ke dalam paket IP. Pemasangan kode pada paket IP tidak dilakukan dengan menambah header baru, tetapi dengan menggantikan 8 bit *field Type of Service (ToS)* pada header IP dengan field *Differentiated Service Code Point (DSCP)* sejumlah 6 bit (2 bit sisa tidak digunakan). Dengan cara ini, klasifikasi melekat pada paket IP dan bisa diakses tanpa perlu protokol tambahan. Jumlah kelas tergantung pada perusahaan dan bukan merupakan standarisasi. Pada trafik lintas batas perusahaan, diperlukan

kontrak trafik yang menyebutkan pembagian kelas dan perlakuan yang diterima untuk setiap kelas. Jika suatu perusahaan tidak mampu menangani skema *Differentiated Service*, maka paket akan dikirim sebagai paket IP biasa, namun di perusahaan berikutnya, skema *Differentiated Service* kembali diakui oleh perusahaan

## METODE PENELITIAN

Metode yang digunakan dalam penelitian ini terdiri dari beberapa tahap, yaitu :

- a. Studi literatur.  
Mengumpulkan informasi dan referensi serta mempelajari tentang konsep jaringan telekomunikasi 3G berbasis IP, arsitektur jaringan perangkat 3G, konsep jaringan TCP/IP dan *Quality of Service (QoS)*.
- b. Analisis dan perancangan sistem.  
Melakukan analisis pada konfigurasi jaringan perangkat telekomunikasi 3G berbasis IP di PT Indosat, Tbk. Cabang Malang dan merancang jaringan simulasi berskala kecil (*testbed*) berdasarkan hasil analisis.
- c. Implementasi sistem.  
Menerapkan konfigurasi hasil perancangan kedalam jaringan *testbed* yang terdiri dari 3 unit komputer, 1 unit *switch* dan 1 unit *router*. Dalam tahap ini juga dipersiapkan *software* aplikasi untuk menjalankan simulasi *traffic* data dan pengukuran *QoS* terhadap penerapan metode *diffserv* pada jaringan TCP/IP tradisional.

- d. Pengambilan data dan analisis hasil pengukuran.  
Menjalankan simulasi *traffic* data serta melakukan pengukuran dan pencatatan terhadap parameter *QoS* yang diujikan.
- e. Penarikan kesimpulan  
Dari hasil analisis pada tahap sebelumnya, ditarik kesimpulan mengenai pengaruh implementasi *diffserv* terhadap *QoS* pada jaringan *testbed* dan kapasitas maksimum *traffic* data yang mampu ditangani oleh jaringan *testbed* ini

## HASIL DAN PEMBAHASAN

### Perancangan Uji Coba Sistem

Lingkungan implementasi yang digunakan dalam penelitian ini meliputi lingkungan perangkat lunak (Software) dan lingkungan perangkat keras (Hardware). Kebutuhan *hardware* (perangkat keras) dalam membangun jaringan *testbed* dalam penelitian ini adalah sebagai berikut :

- 1 unit *router* Cisco 2651 XM dengan spesifikasi 2 Port Fast Ethernet, IOS versi 12.3.
- 1 unit *switch* Cisco Catalyst tipe 2950 dengan spesifikasi 24 Port Fast Ethernet, IOPS versi 12.1.
- 3 unit komputer dengan rincian sebagai berikut :
- 1 komputer sebagai RNC dengan spesifikasi:
  - *Processor* : Intel Core i5
  - *Memory* : 4 GB
  - Sistem Operasi : Windows 7 Ultimate

- 1 komputer sebagai *Node B* dengan spesifikasi :
  - *Processor* : Intel Core i3
  - *Memory* : 4 GB
  - Sistem Operasi : Windows 7 Ultimate
- 1 komputer sebagai *client* aplikasi Wireshark dengan spesifikasi :
  - *Processor* : Intel Core i5
  - *Memory* : 2 GB
  - Sistem Operasi : Windows 7 Home
- 5 buah kabel UTP + konektor RJ45 dengan tipe *straight*.
- USB to Serial *converter* dan kabel *console*.

Kebutuhan *software* (perangkat lunak) dalam mendukung pengujian implementasi *Diffserv* pada jaringan TCP/IP tradisional ini adalah :

#### 1. Wireshark

Aplikasi wireshark digunakan untuk menangkap paket data pada suatu jaringan dengan cara *sniffing*, kemudian melakukan analisis pada tiap *layer* dari paket data yang saling dikirimkan antara *Node B* dan RNC.

#### 2. Ostinato

Ostinato merupakan aplikasi yang berfungsi sebagai *traffic generator* pada saat dilakukan simulasi pengukuran jaringan. Aplikasi ini dijalankan pada komputer yang disimulasikan sebagai *Node B* dan RNC. Karakteristik dari data yang saling dikirimkan dalam simulasi pengukuran dibuat berdasarkan data yang diperoleh melalui aplikasi Wireshark.

#### 3. JPERF

Aplikasi JPERF digunakan untuk mengukur parameter *Quality of Service* berupa

*bandwidth*, *jitter* dan *packet loss* dari jaringan TCP/IP yang disimulasikan.

#### 4. NetPerSec

Aplikasi NetPerSec digunakan untuk menunjukkan jumlah data yang dikirim dan diterima oleh komputer dalam bentuk grafis.

Komponen jaringan TCP/IP yang digunakan sebagai jaringan *testbed* adalah *switch* Cisco Catalyst 2950 dan *router* Cisco 2651 XM. Pada *switch* Cisco Catalyst 2950 dibuat 2 VLAN dengan nama VLAN 837 akan digunakan oleh PC-RNC yang mewakili RNC Malang 2 dan VLAN 102 digunakan oleh PC-*Node B* yang mewakili salah satu VLAN dari 6 *cluster Node B* pada implementasi sebenarnya. Alokasi VLAN, port dan fungsi dari setiap port pada *switch* Cisco Catalyst 2950 ditunjukkan pada tabel 1.

**Tabel 1 Alokasi VLAN, Port dan Fungsi Port Pada Cisco Catalyst 2950**

Device Name	IP address	Default Gateway
PC-Node B	10.234.162.67/26	10.234.162.126/26
PC-RNC	10.253.95.97/29	10.253.95.102/29
Router Port FE 0/0 Sub-If 102	10.234.162.126/26	-
Router Port FE 0/1 Sub-If 837	10.253.95.102/29	-

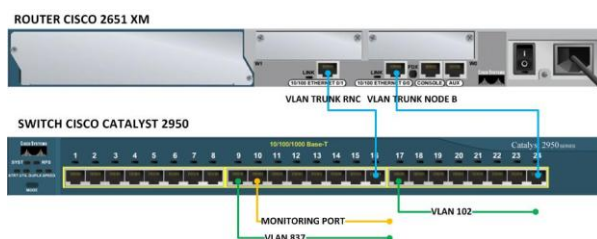


Pengalokasian IP dialokasikan pada PC-RNC, PC-Node B dan *default gateway* pada VLAN trunk yang terdapat pada *router* Cisco 2651 XM. Pada PC-Monitoring tidak perlu dialokasikan alamat IP karena proses *sniffing* dari paket data yang berjalan pada jaringan tersebut dilakukan secara pasif tanpa menggunakan alamat IP. Alokasi alamat IP pada PC-RNC, PC-Node B dan *router* dalam jaringan *testbed* ini ditunjukkan pada tabel.2.

**Tabel 2 Alokasi IP address dan Default Gateway Pada Komputer dan Router**

Port	Type Port	Fungsi
FE 0/9	Access Port	Koneksi ke <i>device</i> PC-RNC
FE 0/10	Monitoring Port	Koneksi ke <i>device</i> PC-Monitoring
FE 0/16	Trunk VLAN 837	Trunk Cisco 2651 XM port FE 0/1
FE 0/17	Access Port	Koneksi ke <i>device</i> PC-Node B
FE 0/24	Trunk VLAN 102	Trunk Cisco 2651 XM port FE 0/0

Koneksi fisik dalam pembentukan jaringan ini membutuhkan 5 buah kabel UTP dengan tipe *straight*, dimana 2 buah kabel digunakan sebagai VLAN *trunk* dari *switch* menuju *router* dan 3 buah kabel digunakan untuk menghubungkan antara *switch* dengan komputer. Gambaran koneksi fisik ditunjukkan pada gambar 4.



**Gambar 4 Koneksi Fisik Pada Jaringan Pengujian (Testbed)**

Konfigurasi pembuatan paket data pada aplikasi *ostinato* menggunakan 4 jenis *traffic* dari PC-Node B menuju PC-RNC dan 3 jenis *traffic* dari PC-RNC menuju PC-Node B. Langkah pertama adalah melakukan *import* data paket IP dari *file* berekstensi *.pcap* yang sebelumnya didapatkan melalui aplikasi *Wireshark*, kemudian paket dimodifikasi sesuai dengan tabel konfigurasi paket data yang telah dirancang. Pada setiap *packet stream* yang akan dijalankan, dilakukan pengaturan ulang pada setiap protocol data, yaitu menggunakan UDP pada layer 4 *protocol* dan *payload* berupa *hexdump*. Parameter Internet Protocol pada setiap *packet stream* diubah sesuai dengan *IP address* komputer asal dan komputer tujuan. Selain menentukan alamat IP, pada menu ini juga dikonfigurasi nilai *Differentiated Service Code Point* (DSCP) dalam bentuk nilai *Type of Service* (ToS) dari 6 bit menjadi 8 bit dengan menambahkan 2 bit dengan nilai 0 pada bit akhir. Setiap paket memiliki *frame length* atau ukuran panjang *frame* yang menentukan besarnya jumlah paket yang ditransmisikan. Perhitungan jumlah paket data yang ditransmisikan didapatkan dengan mengubah satuan *kilobyte* menjadi *byte* kemudian membagi dengan *frame length* dalam *byte* seperti rumus berikut :

$$\text{Packet/second} = \frac{\text{Traffic Data Kilobytes} \times 1024}{\text{Frame Length}}$$

Aplikasi *JPERF* pada pengujian *QoS* dijalankan secara *client-server* dan bergantian antara PC-Node B dan RNC. Tampilan grafik

hasil pengukuran *bandwidth* dan *jitter* serta *packet loss* dalam bentuk *summary* pada *output text* terdapat pada aplikasi JPERF yang dijalankan sebagai *server*. Pengaturan pada sisi client pada menu transport layer options harus sesuai dengan pengaturan yang ada pada *server*. Pengukuran *QoS* jaringan menggunakan *transport layer* UDP secara *default* dengan ukuran *bandwidth* 1 Mbps, *buffer size* 8 byte dan ukuran paket 1470 byte. Pengukuran ini dilakukan selama 60 detik secara bergantian dari PC-Node B menuju PC-RNC dan sebaliknya, maka konfigurasi pada JPERF adalah dengan mengisi 30 detik pada kolom *transmit* dan melakukan check pada menu *trade*.

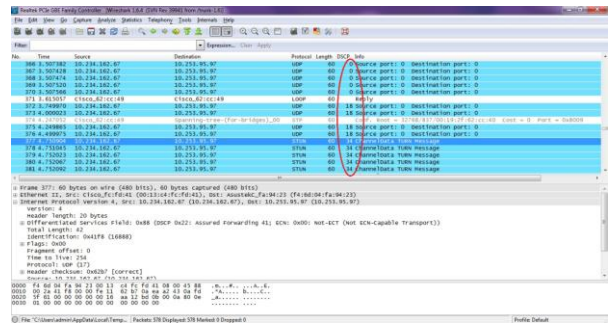
### Pengujian Sistem

Pengujian *QoS* pada jaringan *testbed* dilakukan untuk mengambil nilai *latency*, *jitter* dan *packet loss* pada setiap per hop behaviour (PHB) untuk setiap beban *traffic* data yang disimulasikan.

### Pengujian Packet Capture Dengan Aplikasi Wireshark

Proses ini dilakukan melalui PC-Monitoring dengan aplikasi Wireshark yang terhubung melalui port fast ethernet 0/10 pada *switch* Catalyst 2950 yang dikonfigurasi sebagai SPAN atau *mirroring port*. Pengujian *packet capture* ini dilakukan untuk memastikan bahwa jaringan *testbed* yang terdiri dari *switch* dan *router* tersebut melewatkan paket data dengan prioritas sesuai dengan nilai DSCP serta menjaga konsistensi nilai DSCP tanpa ada modifikasi. Hal ini

ditunjukkan dengan adanya nilai DSCP pada kolom informasi yang tertangkap pada aplikasi ini. Hasil dari proses *packet capture* ditunjukkan pada gambar 5.



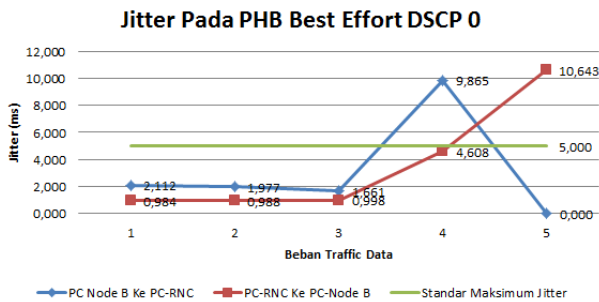
**Gambar 5 Hasil Proses Packet Capture Melalui PC-Monitoring Dengan Aplikasi Wireshark**

Pada gambar 5 terlihat bahwa paket data yang ditangkap memiliki nilai DSCP yang bervariasi yaitu 0, 18, 34 dan 46 menurut jenis *per hop behaviour* (PHB). Hal ini menunjukkan bahwa konfigurasi *switch* dan *router* pada jaringan *testbed* TCP/IP tradisional telah berfungsi sesuai dengan perancangan awal. Jaringan *testbed* ini bekerja tanpa melakukan modifikasi dan membuat nilai DSCP menjadi 0 pada keseluruhan paket data yang melewatinya atau hanya memiliki kelas *best effort* seperti halnya ketika menggunakan konfigurasi *default*.

### Analisis Hasil Pengukuran Jitter

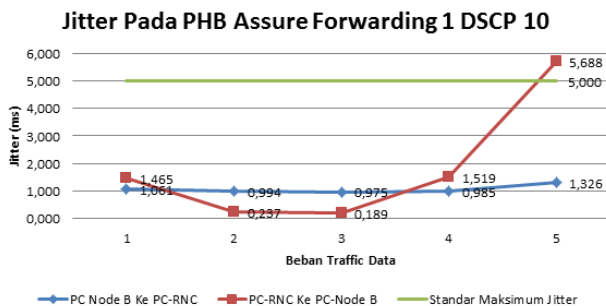
*Jitter* yang merupakan *delay variation* atau variasi waktu kedatangan antar-paket didefinisikan dalam satuan *milisecond* (ms). Nilai *jitter* yang diukur secara *end to end* sesuai standarisasi kualitas jaringan yang ditetapkan oleh PT Indosat, Tbk. adalah kurang dari 5 ms.

Hasil pengukuran pada setiap *per hop behaviour* yang dilakukan dengan beban data yang bertingkat dan dihentikan pada simulasi beban *traffic* data 5. Hal ini dilakukan karena pada tingkat pembebanan data pada jaringan *testbed* telah menunjukkan nilai *jitter* yang melampaui spesifikasi standar.



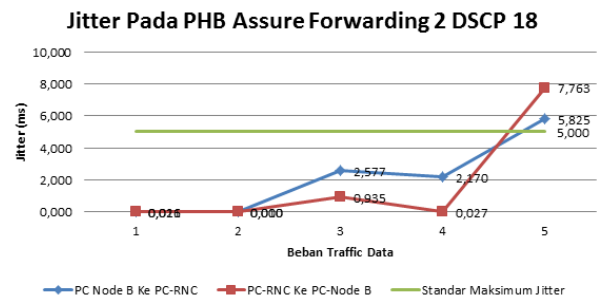
**Gambar 6 Grafik Jitter Pada PHB Best Effort Dengan Beban Traffic Data 1-5**

Seperti yang ditunjukkan pada gambar 6, hasil pengukuran *jitter* pada PHB best effort menunjukkan bahwa dengan simulasi beban *traffic* data 4, *jitter* dari PC-Node B menuju PC-RNC memiliki nilai 9,865 ms di atas nilai standar maksimum *jitter*, sedangkan *jitter* dari PC-RNC menuju PC-Node B menunjukkan nilai 4,608 ms dan masih berada dibawah nilai standar maksimum *jitter*. Pada pengukuran dengan simulasi beban *traffic* data 5, nilai *jitter* dari PC-RNC menuju PC-Node B menunjukkan di atas nilai standar maksimum *jitter* yaitu sebesar 10,643 ms.



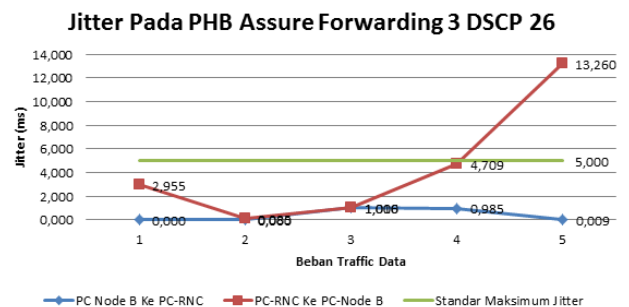
**Gambar 7 Grafik Jitter Pada PHB Assure Forwarding 1 Dengan Beban Traffic Data 1-5**

Nilai *jitter* PC-RNC menuju PC-Node B pada PHB *assure forwarding* 1 seperti yang ditunjukkan pada gambar 7 berada di atas standar maksimum pada saat pengukuran dilakukan dengan simulasi beban *traffic* data 5 yaitu sebesar 5,688 ms. Sedangkan nilai *jitter* PC-Node B menuju PC-RNC relatif stabil dan hingga simulasi pembebanan *traffic* data 5, hasil pengukuran menunjukkan bahwa nilai *jitter* masih berada dibawah standar maksimum yaitu sebesar 1,326 ms.



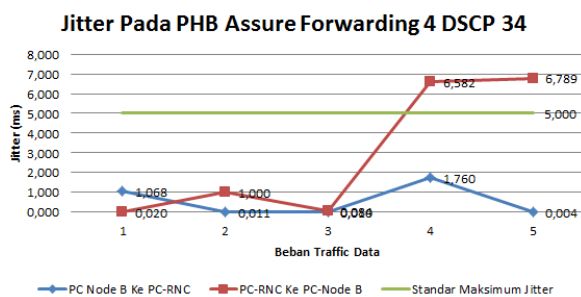
**Gambar 8 Grafik Jitter Pada PHB Assure Forwarding 2 Dengan Beban Traffic Data 1-5**

Pada pengukuran dengan PHB *assure forwarding* 2 seperti yang ditunjukkan gambar 8, nilai *jitter* PC-Node B menuju PC-RNC berada di atas standar maksimum pada simulasi beban *traffic* data 5 yaitu sebesar 7,763 ms dan nilai *jitter* PC-RNC menuju PC-Node B sebesar 5,825 ms.



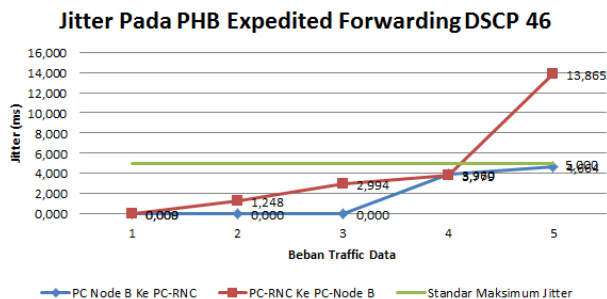
**Gambar 9 Grafik Jitter Pada PHB Assure Forwarding 3 Dengan Beban Traffic Data 1-5**

Pengukuran *jitter* pada PHB *assure forwarding* 3 seperti pada gambar 9 menunjukkan bahwa nilai *jitter* PC-RNC menuju PC-Node B berada diatas standar maksimum yaitu sebesar 13,260 ms pada simulasi beban *traffic* 5. Sedangkan nilai *jitter* PC-Node B menuju PC-RNC masih menunjukkan nilai dibawah standar maksimum hingga simulasi beban *traffic* 5.



**Gambar 10 Grafik Jitter Pada PHB Assure Forwarding 4 Dengan Beban Traffic Data 1-5**

Pada gambar 10 terlihat bahwa nilai *jitter* PC-RNC menuju PC-Node B telah berada diatas standar maksimum pada simulasi beban *traffic* 4 yaitu sebesar 6,582 ms dan pada simulasi beban *traffic* 5 menunjukkan peningkatan menjadi sebesar 6,789 ms. Nilai *jitter* PC-Node B menuju PC-RNC hingga simulasi beban *traffic* 5 tetap berada dibawah standar maksimum *jitter*.



**Gambar 11 Grafik Jitter Pada PHB Expedited Forwarding Dengan Beban Traffic Data 1-5**

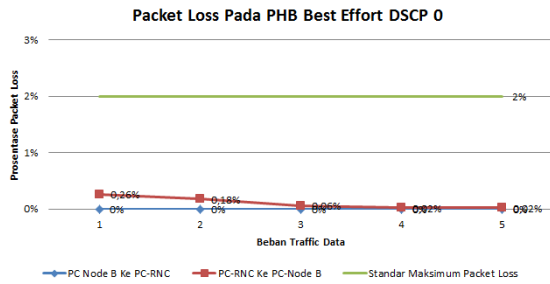
Pengukuran *jitter* pada PHB *expedited forwarding* seperti pada gambar 11 menunjukkan nilai *jitter* PC-RNC menuju PC-Node B melebihi nilai standar pada simulasi beban *traffic* 5 yaitu sebesar 13,865 ms. Nilai *jitter* PC-Node B menuju PC-RNC masih berada dibawah batas maksimum *jitter* pada simulai beban *traffic* 5 yaitu dengan nilai 4,664 ms.

Dengan mempertimbangkan hasil pengukuran *jitter* pada setiap PHB dan tingkatan simulasi beban *traffic* data, maka jaringan *testbed* TCP/IP tradisional ini mampu menjaga *QoS* dengan nilai *jitter* dibawah 5 ms dengan syarat berjalan pada simulasi beban *traffic* 3 atau setara dengan mengoperasikan 3 unit Node B yang terhubung pada 1 RNC. Hal ini disebabkan karena dalam menjalankan simulasi beban *traffic* 4, pada PHB *best effort* dan *assure forwarding* 4 memiliki nilai *jitter* diatas 5 ms yang berarti melebihi standar maksimum yang telah ditetapkan dalam menjaga *Quality of Service*.

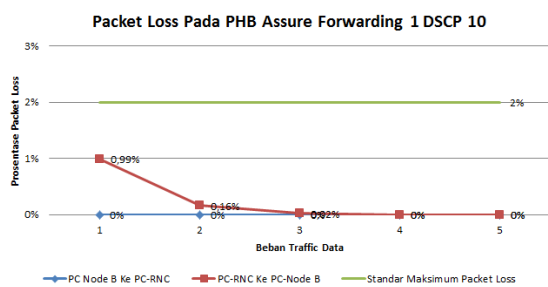
### Analisis Hasil Pengukuran Packet Loss

*Packet loss* yang merupakan kegagalan sebuah jaringan dalam mentransmisikan data dari pengirim menuju penerima dinyatakan dalam prosentase. Nilai prosentase *packet loss* didapatkan melalui pengukuran dengan perhitungan jumlah datagram UDP yang dikirim dengan diterima pada aplikasi JPERF. Prosentase *packet loss* sesuai standar yang telah ditetapkan oleh PT Indosat, Tbk. adalah kurang dari 2%. Grafik hasil pengukuran *packet loss* pada setiap per hop behaviour (PHB) dengan beban *traffic* data 1-5

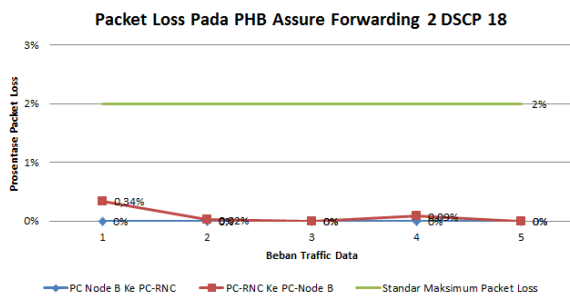
ditunjukkan pada gambar 12 sampai dengan gambar 17.



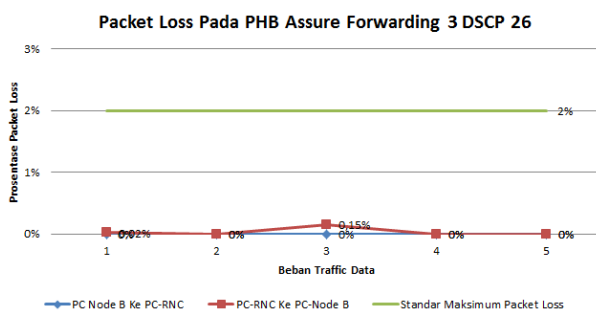
**Gambar 12 Grafik Packet Loss Pada PHB Best Effort Dengan Beban Traffic Data 1-5**



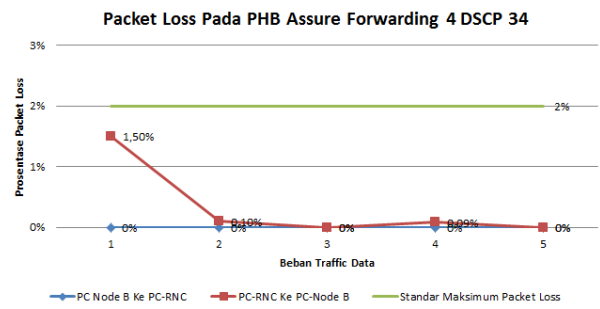
**Gambar 13 Grafik Packet Loss Pada PHB Assure Forwarding 1 Dengan Beban Traffic Data 1-5**



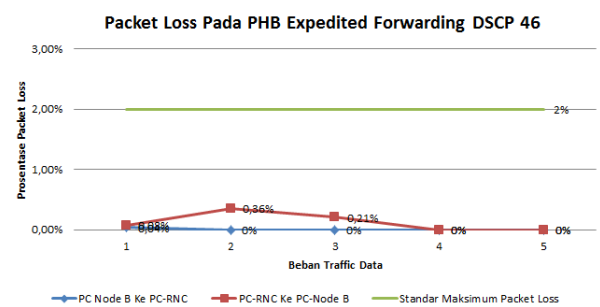
**Gambar 14 Grafik Packet Loss Pada PHB Assure Forwarding 2 Dengan Beban Traffic Data 1-5**



**Gambar 15 Grafik Packet Loss Pada PHB Assure Forwarding 3 Dengan Beban Traffic Data 1-5**



**Gambar 16 Grafik Packet Loss Pada PHB Assure Forwarding 4 Dengan Beban Traffic Data 1-5**



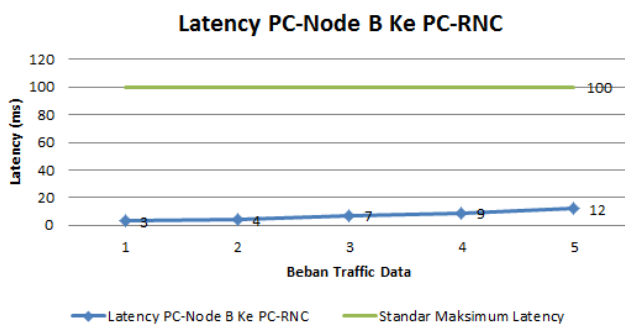
**Gambar 17 Grafik Packet Loss Pada PHB Expedited Forwarding Dengan Beban Traffic Data 1-5**

Berdasarkan hasil serangkaian pengukuran *packet loss* pada setiap *per hop behaviour* (PHB) dengan beban *traffic* data yang bertingkat seperti pada pengukuran *jitter*, nilai *packet loss* yang didapatkan tidak melebihi standar maksimum yang telah ditetapkan.

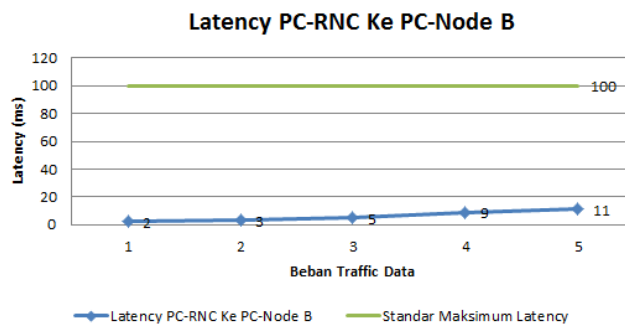
### Analisis Hasil Pengukuran Latency

*Latency* yang merupakan waktu tunda paket data pada proses transmisi dari pengirim menuju penerima data melewati sebuah jaringan diukur dengan melakukan *ping test*. Nilai *latency* dinyatakan dalam *milisecond* (ms) dan memiliki standar batas maksimum kurang dari 100 ms. Pengukuran *latency* dilakukan secara langsung dari *command*

prompt dan tidak dilakukan untuk setiap *per hop behaviour* seperti pada pengukuran *jitter* dan *packet loss*, namun tetap menggunakan beban jaringan yang sama yaitu beban *traffic data* 1 sampai dengan 5. Hasil pengukuran *latency* dari PC-Node B menuju PC-RNC dan sebaliknya ditunjukkan pada gambar 18 dan 20.



**Gambar 18 Grafik Nilai Latency Dari PC-Node B Menuju PC-RNC**



**Gambar 20 Grafik Nilai Latency Dari PC-RNC Menuju PC-Node B**

Berdasarkan grafik pada gambar 18 dan 20 diatas, nilai *latency* pada proses *ping test* dari PC-Node B menuju PC-RNC dan sebaliknya bernilai jauh dibawah standar maksimum *latency* yang ditetapkan. Jaringan *testbed* TCP/IP tradisional ini memiliki nilai *latency* yang relatif kecil karena utilisasi beban jaringan yang disimulasikan belum tinggi hingga menyebabkan *congestion*.

## KESIMPULAN

Berdasarkan hasil pengujian dan analisis dari perancangan jaringan testbed TCP/IP tradisional untuk perangkat telekomunikasi 3G berbasis IP, maka dapat disimpulkan sebagai berikut :

- Metode *diffserv* dapat diaplikasikan pada jaringan TCP/IP tradisional dan mampu memprioritaskan paket data berdasarkan kelas per hop behaviour pada nilai *Differentiated Service Code Point* (DSCP). Hal ini dibuktikan dengan adanya nilai DSCP yang bervariasi yaitu DSCP 0 (*best effort*), 18 (*assure forwarding 2*), 34 (*assure forwarding 4*) dan 46 (*expedited forwarding*) pada proses pengujian packet capture dengan aplikasi Wireshark.
- Kemampuan jaringan TCP/IP tradisional dalam menangani perangkat telekomunikasi Node B di PT Indosat, Tbk dengan tetap menjaga *Quality of Service (QoS)* adalah sejumlah 3 unit Node B yang terhubung pada 1 unit RNC.
- Kendala utama dalam menjaga *QoS* pada jaringan TCP/IP tradisional yang dirancang adalah kemampuan untuk menjaga *jitter* agar tetap dibawah nilai maksimum yang ditetapkan oleh PT Indosat, Tbk. Hal ini dibuktikan dengan nilai *jitter* yang berada di atas standar maksimum pada *per hop behaviour best effort* dan *assure forwarding 4* dalam simulasi beban jaringan yang setara dengan 4 unit Node B. Nilai *packet loss* dan *latency* pada seluruh rangkaian simulasi beban traffic data tetap terjaga dibawah standar nilai maksimum



## DAFTAR PUSTAKA

- Anonymous, 2013. *Overview of The Universal Mobile Telecommunication System*. (<http://www.umtsworld.com/technology/overview.htm> diakses tanggal 2 Juli 2013).
- Anonymous, 2013. *Multi Protocol Label Switching FAQ for Beginners*. ([http://www.cisco.com/en/US/tech/tk436/tk428/technologies\\_q\\_and\\_a\\_item09186a00800949e5.shtml#qa6](http://www.cisco.com/en/US/tech/tk436/tk428/technologies_q_and_a_item09186a00800949e5.shtml#qa6) diakses tanggal 3 Juli 2013).
- Anonymous, 2013. *Iperf – The TCP/UDP Bandwidth Measurement Tool*. (<http://iperf.fr> diakses tanggal 5 Juli 2013).
- C.Y.Lee, William. 2006. *Wireless & Cellular Telecommunications. Third Edition*. New York: McGraw Hill.
- Cisco System. 2013. *Implementing Quality of Service Policies with DSCP*. ([http://www.cisco.com/en/US/tech/tk543/tk757/technologies\\_tech\\_note09186a00800949f2.shtml](http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml) tanggal 12 Juli 2013).
- Cisco System. 2013. *Configuring Class-Based Packet Marking*. ([http://www.cisco.com/en/US/docs/ios/12\\_2/qos/configuration/guide/qcfcbmrk.html](http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcbmrk.html) tanggal 12 Juli 2013).
- Cisco System. 2013. *Diffserv - The Scalable End-to-End QoS Model*. ([http://www.cisco.com/en/US/technologies/tk543/tk766/technologies\\_white\\_paper09186a00800a3e2f.html](http://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.html) tanggal 12 Juli 2013).
- E. Flannagan, Michael. 2001. *Administering Cisco QoS*. Rockland: Syngress Publishing, Inc.
- Hundley, Kent. 2009. *Alcatel-Lucent Scalable IP Networks Self-Study Guide*. Indianapolis: Wiley Publishing, Inc.
- Krismiaji. 2005. *Sistem Informasi Akuntansi*. Yogyakarta: Unit Penerbit dan Percetakan Akademi Manajemen Perusahaan YKPN.
- Lukas, Jonathan. 2006. *Jaringan Komputer*. Yogyakarta: Graha Ilmu.
- Richasse, Nicolas P. 2013. *XJPERF Graphical Frontend for IPERF Written in Java*. (<http://code.google.com/p/xjperf/> tanggal 04 Juli 2013).
- Srivats P. 2013. *Ostinato Packet/Traffic Generator and Analyzer*. (<http://code.google.com/p/ostinato> tanggal 05 Juli 2013).
- Wang, Zheng. 2001. *Internet QoS Architectures and Mechanism for Quality of Service*. San Fransisco: Morgan Kaufmann Publishers.