

PENGGUNAAN TEKNOLOGI KOMUNIKASI DATA BERBASIS VPN-IP MPLS UNTUK PEMILIHAN UMUM

Rijal Fadilah¹⁾, Djumhadi²⁾

^{1,2)}Jurusan Teknik Informatika, STMIK Balikpapan
Jl. K.P Tendean 2A Gunung Pasir Balikpapan Kalimantan Timur
Telp. 0542-7070213, Faks. 0542-424545
e-mail: rijalf@gmail.com

Abstrak

Dalam setiap tahapan pemilihan umum baik untuk pemilihan anggota legislatif hingga pemilihan presiden berbagai proses harus ditempuh. Dimulai dari pendaftaran pemilih, pencalonan partai politik, pencalonan anggota DPR/DPRD, pencalonan DPD, kampanye, pemungutan suara, perhitungan suara hingga penetapan hasil Pemilu. Tentu saja yang sangat dinantikan adalah proses penghitungan suara. Tahapan ini menjadi tahapan yang menegangkan bagi setiap konsisten yang ikut berlaga di pemilihan umum. Sebagai suatu proses yang menegangkan dan dinantikan banyak pihak diperlukan keakuratan dan kecepatan dalam proses penghitungan tersebut dan tidak kalah pentingnya adalah hasil penghitungan suara dapat disampaikan ataupun dikirimkan dari masing-masing daerah ke pusat dengan aman, fleksibel dan mudah dipantau dari segi komunikasi datanya.

Teknologi Virtual Private Network yaitu jaringan pribadi yang tidak bisa diakses oleh jaringan nonpribadi namun menggunakan medium nonpribadi semisal internet untuk menghubungkan antar masing-masing titik (remote site) secara aman. Dalam penggunaan teknologi Virtual Private Network perlu penerapan teknologi tertentu sehingga meskipun menggunakan medium yang umum, tetapi traffic (lalu lintas) antar remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidak semestinya ke dalam remote-site. IP-MPLS (Internet Protocol-Multi Protocol Label Switching) merupakan layanan komunikasi data dalam bentuk dedicated leased channel berbasis IP dengan keunggulan utama any to any connection yang dapat disesuaikan dengan jenis traffic yang dilewatkan.

Dalam implementasinya VPN-IP MPLS dapat dikembangkan menjadi berbagai fitur antara lain : Intranet, Extranet, serta Remote Dial. Teknologi ini memiliki beberapa kentungan seperti : Multiservices Platform, Scalability, Manageability serta Cost Saving Opportunity.

Keywords: VPN IP-MPLS, Private Network, Pemilihan Umum

1. PENDAHULUAN

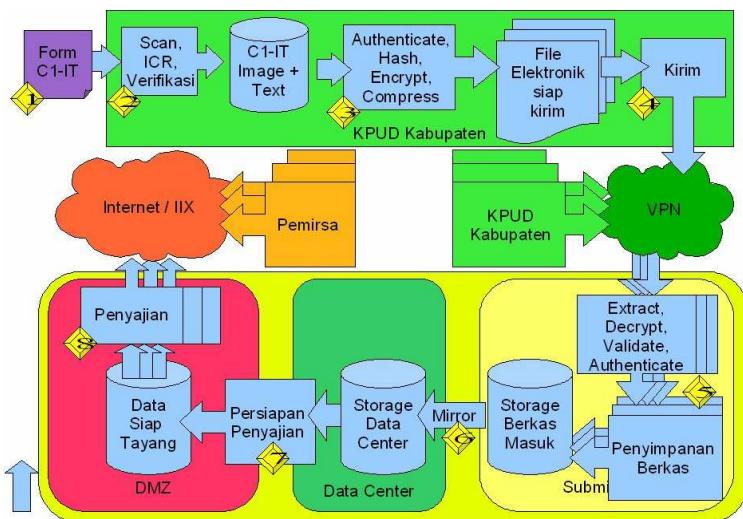
Berbagai kalangan menilai bahwa sistem informasi dan teknologi yang diterapkan oleh Komisi Pemilihan Umum (KPU) untuk Pemilihan Umum (PEMILU) 2009 memang termasuk cukup canggih, namun cukup disesalkan pula karena jumlah server yang disediakan tidak sebanding dengan data yang diupload. Sistem yang diterapkan saat ini berbeda dibandingkan PEMILU 2004 lalu, dimana pada proses tabulasi langsung dilakukan secara online dari berbagai wilayah dan bisa segera terlihat hasilnya. Sedangkan dalam PEMILU 2009 Komisi Pemilihan Umum (KPU) menggunakan teknologi ICR (*Intelligent Character Recognition*). ICR pada dasarnya merupakan suatu sistem yang mampu mengenali tulisan tangan dan menterjemahkannya ke dalam kode atau simbol digital sehingga data dapat dimengerti oleh komputer. Terdapat beberapa bagian penting yang terkandung dalam ICR ini, antara lain *preprocessing*, *character segmentation*, *character recognition*.

Preprocessing merupakan teknik dalam pengolahan citra guna meningkatkan kualitas gambar sehingga memudahkan untuk melakukan proses selanjutnya. Lalu *character segmentation* bertugas menganalisa sebuah citra teks hasil *scanning*, lalu menemukan lokasi teks dan mengekstrak huruf per huruf untuk diolah pada tahap *character recognition*. *Character recognition* sendiri terdiri dari *feature extraction* dan *classification* yang bertugas menemukan informasi yang signifikan dari citra sebuah huruf dan merepresentasikannya dalam vektor fitur. Kemudian vektor tersebut diolah oleh *classifier* guna menentukan berbagai jenis huruf yang ada. Seperti diketahui proses perhitungan suara pada PEMILU 2009 ini, KPU telah membuat kesepakatan dengan berbagai pihak bahwa teknologi yang digunakan adalah ICR. Maka untuk menguatkan penggunaan teknologi tersebut, KPU telah menetapkan peraturan KPU No. 02 Tahun 2009. Dalam pertaturan tersebut disebutkan dengan perangkat lunak ini diharapkan akan mempercepat proses perhitungan suara, memperoleh tabulasi yang akurat, memperoleh salinan dokumen elektronik yang otentik, aman dan transparan. Jika kita perhatikan halaman Website KPU (<http://tnp.kpu.go.id>) yang menampilkan update data suara sering terasa lambat, dari menit ke menit terasa lambat. Sebenarnya dari sisi teknologi, ICR bukanlah hal baru, dimana riset mengenai *character recognition* telah lama digunakan para peneliti di dunia komputasi, khususnya dalam pengenalan pola dan pengolahan citra. Jadi dari sisi teknologi ICR memang sudah teruji dan telah banyak diimplementasikan.

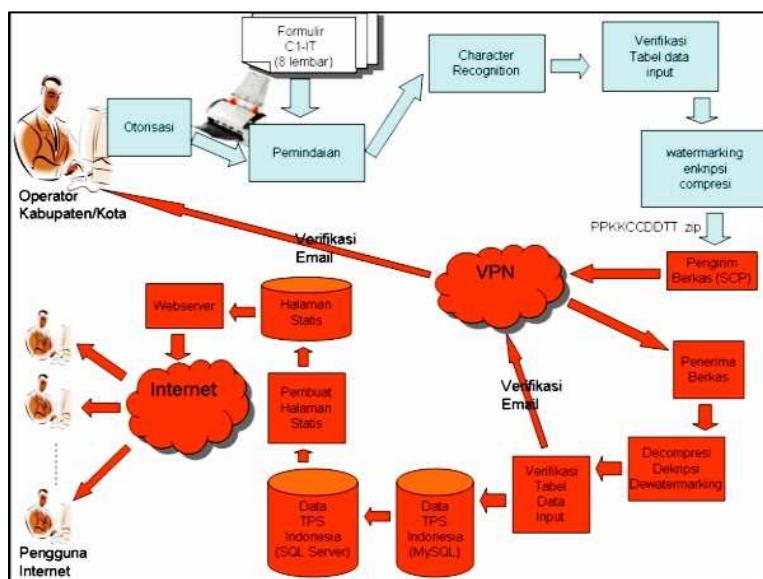
Kalau kita cermati sejak tanggal 9 April 2009 lalu, gelombang protes, berbagai pengaduan dan lain-lain sudah terjadi di berbagai tingkatan. Melihat kenyataan tersebut proses perhitungan suara ini cukup beresiko,

dilihat dari banyaknya partai politik yang ikut bertarung dan banyaknya masalah sebelum pelaksanaan PEMILU itu sendiri bisa menjadi pemicu. Sebagai contoh, hampir tiap malam televisi menyiarkan jumlah pemilih fiktif, Daftar Pemilih Tetap (DPT) amburatul, dan sebagainya. Bahkan yang paling riskan adanya sekelompok yang merasa tidak puas dengan hasil perhitungan suara termasuk di beberapa daerah yang minta perhitungan suara ulang, pemilu susulan, dan sebagainya.

Secara singkat arus data dan informasi dalam sistem informasi yang diterapkan oleh KPU untuk mendukung Pemilu 2009 tergambar dalam ilustrasi berikut:



Gambar 1. Ilustrasi Alur Data Sistem Teknologi Informasi PEMILU 2009



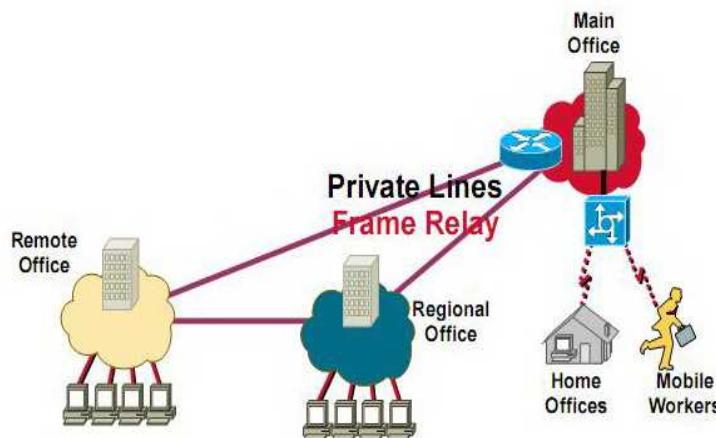
Gambar 2. Bagan Alur Data Sistem Teknologi Informasi PEMILU 2009

Lalu bagaimana dengan sistem komunikasi data yang dipergunakan untuk mendukung sistem teknologi informasi ini? Makalah ini mencoba memaparkan secara singkat tentang sistem komunikasi data yang dipergunakan oleh KPU baik di Pusat maupun di daerah, KPU maupun KPUD.

2. TINJAUAN PUSTAKA

Solusi sistem informasi terintegrasi memerlukan infrastruktur komunikasi data, teknologi yang sering disebut *Wide Area Network (WAN)* atau jaringan skala luas. Ada banyak solusi yang bisa digunakan untuk komunikasi data pada jaringan skala luas, saat ini terdapat beberapa solusi komunikasi data yang ditawarkan provider telekomunikasi. WAN adalah jaringan komunikasi yang meliputi area geographis yang luas dan biasanya menggunakan fasilitas dari transmisi provider, seperti perusahaan telekomunikasi atau lainnya.

Infrastruktur inilah yang nantinya menjadi penghubung antara kantor pusat ke cabang-cabang dan *telecommuters*. Selain sistem informasi yang kita bangun, infrastruktur harus menjadi perhatian khusus dalam penggunaan solusi teknologi informasi yang akan dibangun. Ada beberapa hal yang harus diperhatikan dalam memilih solusi infrastruktur jaringan komunikasi ini, diantaranya : *bandwidth, technology, scalability, support IP based, easy configuration and maintenance, low cost and security*. Menurut hasil penelitian dari infonetics dalam <http://www.byteandswitch.com> dikatakan bahwa saat ini penggunaan interkoneksi WAN meningkat 58% pada kuartal pertama tahun 2007 dan kuartal pertama tahun 2008.



Gambar 3. Topologi Classic WAN

Seperti pada gambar 3 terlihat topologi yang sering dahulu digunakan untuk mengkoneksikan banyak kantor cabang dan para pekerja yang *mobile* menggunakan infrastruktur penyedia jasa leased line, frame relay, dial-up atau menggunakan *ATM (Asynchronous Transfer Mode)*, namun karena ketidakseimbangan antara tingginya biaya yang harus dikeluarkan dengan rendahnya kemampuan teknis (bandwidth, protocol, interface, lastmiles, coverage area, jarak dan lain-lain) maka solusi WAN classic ini mulai ditinggalkan.

Seiring dengan perkembangan teknologi yang makin membuat semua mudah dan murah, tidak terkecuali berpengaruh besar terhadap teknologi telekomunikasi. Contohnya jaringan yang berbasiskan *IP (Internet Protocol)* yang kini merupakan wujud tata dunia baru (*new world*). Jaringan *IP* kini memungkinkan para pelaku bisnis maupun instansi menjalankan bisnis dan pekerjaannya dengan suatu cara yang jauh lebih efisien, efektif, dan murah tetapi andal. Kemampuan teknologi *IP* membangun jaringan internet dalam skala besar dan tingkat keandalan tinggi merupakan salah satu modal utama untuk memberikan layanan komunikasi baru, *VPN-IP (Virtual Private Network-IP)*.

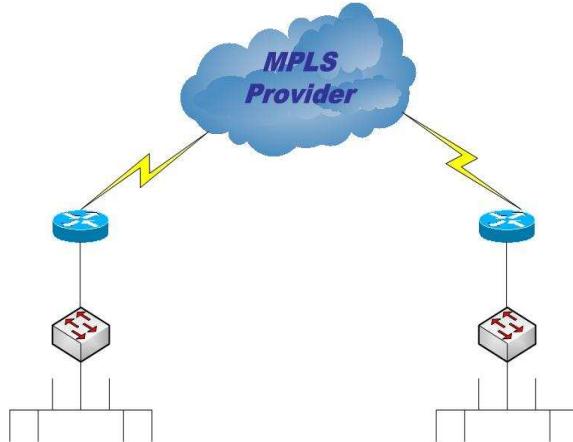
VPN-IP mengkombinasikan berbagai unsur dalam teknologi *IP* untuk memberi layanan yang memenuhi berbagai komponen layanan komunikasi baku yang ditawarkan oleh teknologi sebelumnya. Semisal yang ditawarkan oleh saluran sewa (*leased line*), *frame relay* dan *ATM (Asynchronous Transport Mode)*. Komponen-komponen layanan komunikasi itu, menurut Achmad Sugiarto, GM Datakom Divisi Multi Media PT Telkom (2005), antara lain keandalan, jangkauan, dan keamanan penggunaan. Teknologi *VPN-IP* memiliki tingkat fleksibilitas yang lebih baik dibandingkan dengan *leased line*, *frame relay*, maupun *ATM*, dan juga menawarkan solusi yang lebih murah.

Hasil penelitian *InternetWeek Research* memperlihatkan bahwa alasan utama para manajer teknologi informasi (TI) memilih teknologi *VPN-IP* dibandingkan dengan teknologi lainnya adalah untuk mengurangi biaya komunikasi yang cukup tinggi. Alasan ini merupakan dasar yang kuat bagi manajer TI untuk menggunakan layanan *VPN-IP* karena tidak perlu waktu berlama-lama untuk mendapat persetujuan dari manajemen. Lebih dari separuh manajer TI yang diteliti mengatakan bahwa mereka telah dan akan menggunakan layanan *VPN-IP* dalam waktu enam bulan ke depan dan merencanakan semua layanan komunikasi seperti Intranet, extranet, Internet voice, e-commerce, dan aplikasi multimedia lainnya yang akan diintegrasikan dengan layanan *VPN-IP*.

Suatu jaringan idealnya dapat menghubungkan antartik secara *any to any*. Di masa lalu, perusahaan yang hendak menghubungkan cabang-cabang kantornya dalam suatu jaringan akan menggunakan saluran sewa secara titik ke titik (*point to point*) yang tentu saja biayanya sangat besar. Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan Internet sebagai bagian dari jaringan mereka untuk menghemat biaya. *VPN* adalah salah satu cara untuk membuat sambungan *any to any* di atas jaringan publik seperti Internet, tanpa klien yang satu dengan klien yang lain saling mengetahui.

Dewasa ini ada dua teknik yang dikenal untuk mengembangkan *VPN* di atas jaringan Internet yaitu *Internet Protocol Security* yang disingkat dengan *IPSec*, dan *Multiprotocol Label Switching (MPLS)*. Dua kelompok kerja di *Internet Engineering Task Force (IETF)* telah memfokuskan diri pada mekanisme keamanan

di Internet, standarisasi label switching dan mutu layanan (*Quality of Services/QoS*) yang berhubungan dengan arsitektur *VPN*. Kelompok kerja *IPSec* (di bawah area keamanan) berkonsentrasi pada proteksi lapisan jaringan dengan merancang mekanisme keamanan pengacakan (kriptografi). Mekanisme ini ujar Achmad Sugiarto (2005), secara fleksibel dapat mendukung kombinasi dari otentifikasi, integritas, kontrol akses, dan kerahasiaan. Adapun kelompok kerja *MPLS* yang berada di bawah area routing, di sisi lain mengembangkan mekanisme untuk mendukung higher layer resource reservation, *QoS* dan definisi perilaku host. Para penyedia jasa biasanya menawarkan salah satu di antara kedua arsitektur jaringan ini berdasarkan kebutuhan pelanggan dan pasar yang dilayani.



Gambar 4. Konfigurasi Umum VPN IP MPLS

Dengan fleksibilitas jaringan IP yang sangat tinggi maka berbagai macam layanan dan aplikasi dapat dijalankan di atas jaringan sistem IP MPLS. Layanan dari tingkat integritas dan interaktivitas tinggi seperti video, voice dan data tertentu sampai dengan layanan non-critical dan non-delay sensitive seperti layanan internet dan E-mail dapat secara optimal dilayani dalam satu jaringan fleksibel IP MPLS. Beberapa fitur IP MPLS antara lain:

a. Intranet

Jaringan Intranet umumnya terdiri atas berbagai aplikasi yang kemudian dibawa dalam bentuk bermacam-macam jenis trafik pula. IP MPLS dengan kemampuan CoS-nya sangat sesuai untuk digunakan sebagai jaringan aplikasi semacam ini.

b. Extranet

Faktor terpenting dalam jaringan extranet adalah security dan accessabilitiy. IP MPLS mendukung kedua requirement ini. Sistem keamanan selain telah dijamin di dalam core network IP MPLS dalam bentuk VPN untuk setiap group pemakai, di sisi pemakai masih dapat ditambah firewall atau sistem keamanan lain seperti enkripsi, dan lain-lain. Dalam hal accessabilitiy jaringan IP memiliki kemampuan penuh untuk dapat dipergunakan oleh berbagai aplikasi.

c. Remote Dial

Faktor accessability dapat dijawab pula dengan *remote dial system* dalam jaringan IP MPLS. *System remote dial* ini dapat pula diaplikasikan dalam bentuk VPN Dial yang dapat mengintegrasikan berbagai jaringan termasuk IP MPLS, *Frame Relay* dan jenis LC (*Leased Channel*) lainnya.

3. METODE PENELITIAN

Untuk membahas topik tentang komunikasi data dengan VPN IP MPLS dilakukan dengan cara :

a. Studi literatur

Tujuan utama dalam melakukan studi literatur dalam penelitian ini adalah :

1. Menemukan variabel-variabel yang akan diteliti.
2. Membedakan hal-hal yang sudah dilakukan dan menentukan hal-hal yang perlu dilakukan
3. Melakukan sintesa dan memperoleh perspektif baru
4. Menentukan makna dan hubungan antar variabel

Beberapa sumber yang digunakan oleh peneliti di antaranya:

1. Abstrak hasil penelitian
2. Indeks

3. Review
 4. Jurnal
 5. Buku referensi
- b. Studi lapangan
Merupakan desain penelitian yang mengkombinasikan antara studi literatur, survei berdasarkan pengalaman dan atau studi kasus dimana peneliti berusaha mengidentifikasi variabel-variabel penting dan hubungan antar variabel tersebut dalam suatu situasi permasalahan tertentu. Studi lapangan ini digunakan sebagai sarana penelitian lebih lanjut dan mendalam.
Dalam penelitian ini studi lapangan yang dilakukan adalah memantau dan mengamati penggunaan layanan VPN IP yang digunakan untuk komunikasi data Pemilu 2009 dari segi konfigurasi fisik dan logik layanan, khususnya di wilayah Kalimantan Timur dan Kalimantan Selatan. Keterbatasan ini terkait dengan wilayah domisili peneliti.
- c. Wawancara
Wawancara merupakan tanya jawab langsung antara peneliti dengan narasumber sebagai responden, khususnya mengenai masalah yang diajukan secara khusus oleh peneliti. Studi ini dilakukan oleh peneliti dalam rangka untuk menemukan kasus-kasus khusus yang perlu diketahui.
Dalam penelitian ini wawancara dilakukan kepada salah satu personal yang terlibat langsung dalam penyedia layanan VPN IP untuk Pemilu 2009 baik dari sisi provider maupun personil petugas di lapangan yang menggunakan layanan ini.

4. HASIL DAN PEMBAHASAN

Untuk implementasi sistem teknologi informasi PEMILU 2009 ini, PT. Telkom Indonesia kembali menjadi penyedia fasilitas telekomunikasi (Fastel) untuk Pemilu 2009 setelah melalui tender terbuka yang diselenggarakan Komisi Pemilihan Umum. Sebagai pemenang tender, Telkom harus menyediakan bandwidth, instalasi, integrasi, fasilitas *Disaster Recovery Center (DRC)*, *Layanan Call Center* serta layanan Pemeliharaan Jaringan.

Menurut Pontjo W. Nugroho, Kepala Proyek Fastel Pemilu 2009, ada beberapa alokasi pekerjaan terkait tender ini. Alokasi tersebut termasuk di Kantor KPU Pusat di Jakarta, 504 Kantor KPU Kota/Kabupaten serta di lokasi DRC di Serpong. Secara ringkas detail layanan yang disediakan Telkom adalah sebagai berikut:

1. Di Kantor KPU Pusat, Telkom menyediakan back haul Data Center VPN-IP kapasitas 30 Mbps yang melalui link *Fibre Optic (FO)*
2. Link Data Center dan fasilitas *Disaster Recovery Center (DRC)*, Metro Ethernet kapasitas 10 Mbps melalui link *Fibre Optic (FO)*
3. Layanan Call Center khusus Pemilu 0800-1-PEMILU, penyediaan infrastruktur dan akses Call Center hingga Aplikasi Network Monitoring.
4. Kantor KPU Kota/Kabupaten, Telkom menghadirkan *Connectivity End Point VPN-IP* nirkabel (*DSLAM & TDM*) atau berbasis *VSAT*. Menempatkan seorang teknisi di setiap lokasi kantor KPU yang bertugas menangani masalah koneksi yang mungkin terjadi.
5. Untuk *Disaster Recovery Centre* yang berada di German Center, Bumi Serpong Damai, Serpong, layanan Telkom mencakup VPN-IP 30 Mbps melalui link *Fibre Optic (FO)*, *Collocation Server*, Penyediaan unit server, router, firewall dan mirroring application, *setup connectivity* antara *Disaster Recovery Centre* dengan *back haul* dan dengan *end point* 504 lokasi KPU Kota/Kabupaten.

Tabel berikut menyajikan data teknis untuk layanan VPN IP PEMILU pada KPU Pusat dan KPUD di wilayah Kalimantan Timur dan Kalimantan Selatan:

Tabel 1. Data Teknis VPN IP untuk KPU Pusat

| Nama KPU | Lokasi | IP Modem | Router PE | IP LAN | IP WAN |
|-------------------------|---------|-------------|--------------------------|---------------|--------------------|
| KPU Pusat (Backhaul) | Jakarta | 172.16.10.0 | PE2-D2-GB2 Gi4/7.2021 | 10.10.10.0/24 | 192.169.146.144/30 |

Tabel 2. Data Teknis VPN IP untuk KPU di wilayah Kalimantan Timur dan Kalimantan Selatan

| Nama KPUD | Lokasi | IP Modem | Router PE | IP LAN |
|------------------------------------|---------------|----------------|------------------------|------------------|
| Provinsi Kalimantan Timur | | | | |
| Kabupaten Pasir | Tanah Grogot | 172.21.52.7 | PE-D6-TGT Fa0/1.703 | 10.100.31.17/28 |
| Kabupaten Kutai Kartanegara | Tenggarong | 10.36.79.4 | PE2-D6-TGG Gi0/3.1201 | 10.100.31.33/28 |
| Kabupaten Berau | Tanjung Redeb | 172.18.214.136 | PE-D6-TJR Fa0/1.725 | 10.100.31.49/28 |
| Kabupaten Bulungan | Tanjung Selor | 172.21.54.8 | PE-D6-TJS Gi0/2.707 | 10.100.31.65/28 |
| Kabupaten Nunukan | Nunukan | 172.26.151.136 | PE-D6-TRK Gi0/1.906 | 10.100.31.81/28 |
| Kabupaten Malinau | Malinau | 172.21.50.4 | PE-D6-TRK Gi0/1.721 | 10.100.31.97/28 |
| Kabupaten Kutai Barat | Melak | 10.36.12.5 | PE-D6-MLK Gi0/3.1201 | 10.100.31.113/28 |
| Kabupaten Kutai Timur | Sangatta | | PE-D6-SGT Se4/0:3 | 10.100.31.129/28 |
| Kota Balikpapan | Balikpapan | | PE4-D6-BPP Se3/2:2 | 10.100.31.144/28 |
| Kota Samarinda | Samarinda | 172.16.155.120 | PE2-D6-SMD Fa0/1.715 | 10.100.31.161/28 |
| Kota Tarakan | Tarakan | 172.18.206.192 | PE-D6-TRK Gi0/1.814 | 10.100.31.177/28 |
| Kota Bontang | Bontang | 172.26.153.132 | PE-D6-BOG Gi0/1.903 | 10.100.31.193/28 |
| Kabupaten Penajam Paser Utara | Penajam | 172.26.148.144 | PE-D6-BPP Gi0/1.948 | 10.100.31.209/28 |
| Kabupaten Tana Tidung | Malinau | 10.36.78.3 | PE-D6-TRK Gi0/1.1201 | 10.100.31.225/28 |
| Provinsi Kalimantan Selatan | | | | |
| Kabupaten Tanah Laut | Pelaihari | -- | PE-D6-BJM Se3/3:1 | 10.100.32.16/28 |
| Kabupaten Kota Baru | Kota Baru | -- | VSAT IP | -- |
| Kabupaten Banjar | Martapura | 172.21.90.5 | PE-D6-BJB Gi0/1.713 | 10.100.32.49/28 |
| Kabupaten Barito Kuala | Marabahan | 172.23.104.10 | PE-D6-BJM PE Gi0/2.777 | 10.100.32.65/28 |
| Kabupaten Tapin | Rantau | 172.23.102.10 | PE-D6-BJM Gi0/2.797 | 10.100.32.81/28 |
| Kabupaten Hulu Sungai Selatan | Kandangan | 172.25.88.11 | PE-D6-KGN Et2/0.707 | 10.100.32.97/28 |
| Kabupaten Hulu Sungai Tengah | Sungai Tengah | 172.21.84.11 | PE-D6-KGN Fa0/1.737 | 10.100.32.113/28 |
| Kabupaten Hulu Sungai Utara | Amuntai | 172.23.101.7 | PE-D6-BJM Gi0/2.754 | 10.100.32.129/28 |
| Kabupaten Tabalong | Tabalong | 172.25.70.11 | PE-D6-TJT Fa0/1.708 | 10.100.32.145/28 |
| Kabupaten Banjar Baru | Banjarbaru | 172.26.141.194 | PE-D6-BJM Gi0/2.967 / | 10.100.32.161/28 |
| Kota Banjarmasin | Banjarmasin | 172.26.141.192 | PE-D6-BJM Gi0/2.966 | 10.100.32.177/28 |
| Kabupaten Tanah Bumbu | Batulicin | 10.36.81.3 | PE-D6-BLN Gi0/1.700 | 10.100.32.192/28 |
| Kabupaten Balangan | Balangan | -- | PE-D6-TJT Se1/0:6 | 10.100.32.209/28 |

Adapun data konfigurasi backhaul layanan VPN IP Pemilu 2009 di router PE adalah sebagai berikut:

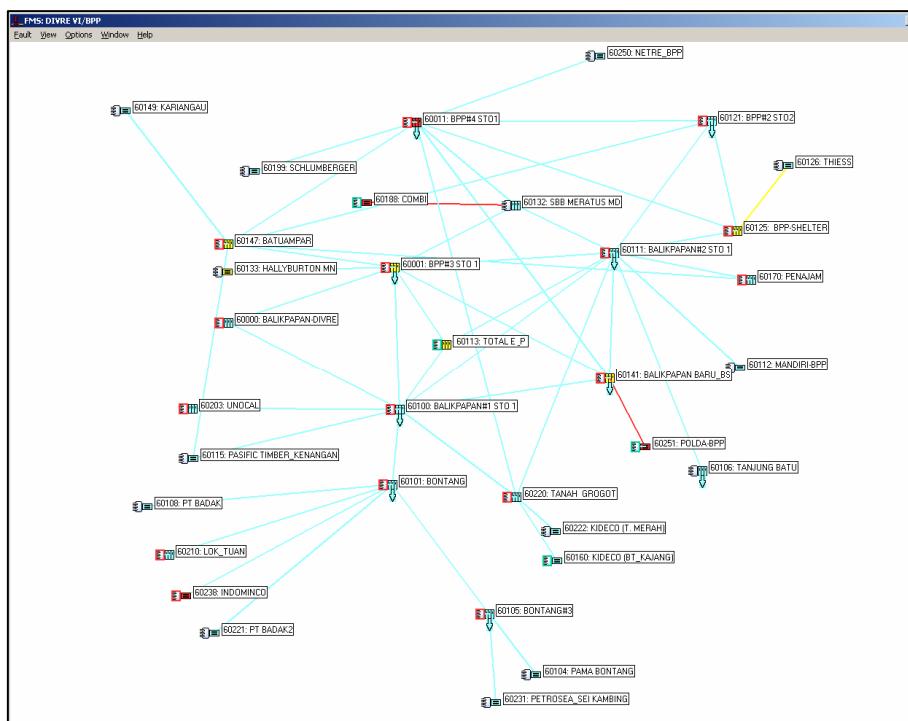
```
GigabitEthernet4/7.2021 is up, line protocol is up (connected)
Hardware is C6k 1000Mb 802.3, address is 001b.0ded.8e40 (bia 001b.0ded.8e40)
Description: VPNIP KPU/PROPINI DKI JAKARTA BACKHAUL CID 4707079-44864
Internet address is 192.169.146.145/30
MTU 1500 bytes, BW 30720 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 2021.
ARP type: ARPA, ARP Timeout 04:00:00
```

Pada data tabel 1 dan tabel 2 di atas dapat dilihat berbagai *interface* yang digunakan untuk menghubungkan masing-masing *end point* ke *cloud MPLS* milik provider Telkom. Secara ringkas kecepatan ethernet disajikan dalam tabel berikut:

Tabel 3. Spesifikasi Ethernet

| Nama Umum | Standar IEEE | Kecepatan |
|----------------------------|--------------|-----------|
| Ethernet | 802.3 | 10 Mbps |
| Fast Ethernet | 802.3u | 100 Mbps |
| Gigabit Ethernet (Optical) | 802.3z | 1 Gbps |
| Gigabit Ethernet (Tembaga) | 802.3ab | 1 Gbps |
| 10 Gigabit Ethernet | 802.3ae | 10 Gbps |

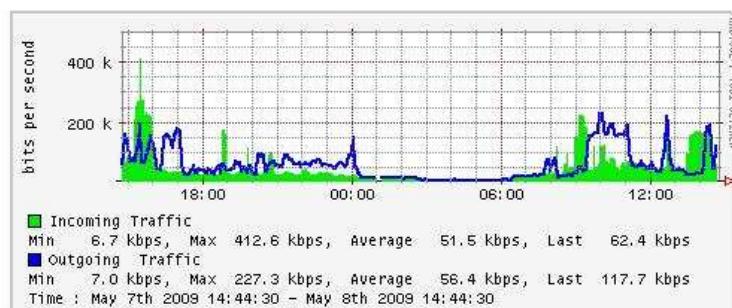
Dalam hal *manageability* layanan, untuk *End to End Manageability* dipantau dalam suatu NMS (*Network Monitoring System*) yang terpadu dan terpusat. Semua *network* elemen dapat dipantau dan di program secara remote dari NMS pusat ini. Integritas ini menjamin kecepatan service recovery dan sistem pelaporan performansi jaringan apabila dibutuhkan.



Gambar 5. Capture NMS (*Network Monitoring System*)

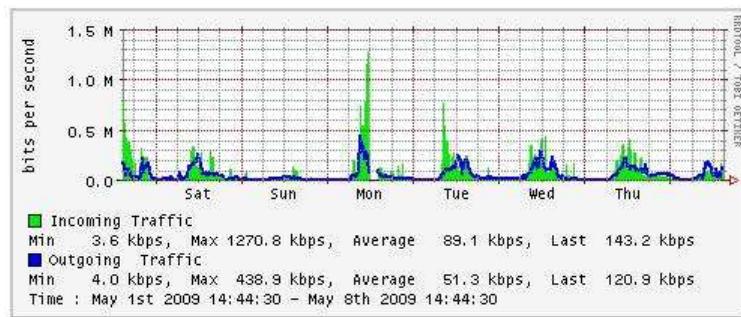
Untuk memantau *traffic* dipergunakan aplikasi MRTG (*Multi Router Traffic Grapher*), merupakan aplikasi yang digunakan untuk memantau beban trafik pada *link* jaringan. MRTG akan membuat halaman HTML (berbasis web) berisi gambar GIF yang menggambarkan trafik melalui jaringan secara harian, mingguan, bulanan dan tahunan. Gambar Berikut ini menyajikan *capture traffic* pemakaian yang terekam pada sistem MRTG.

Daily Graph



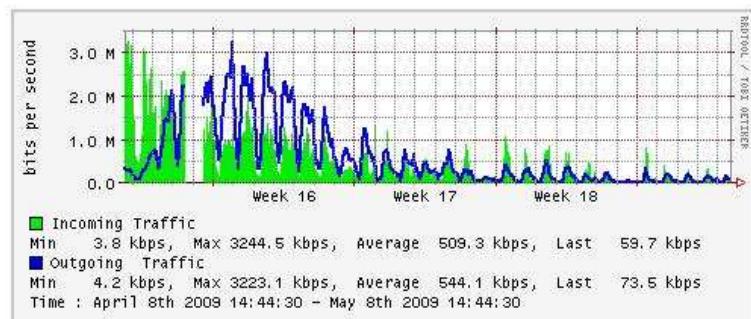
Gambar 6. Capture Traffic Back Haul VPN IP KPU Pusat pada tanggal 8 Mei 2009
(Sumber: www.mrtg.telkom.net)

Weekly Graph



Gambar 7. Capture Traffic Back Haul VPN IP KPU Pusat dari tanggal 1 Mei 2009 s.d 8 Mei 2009
(Sumber: www.mrtg.telkom.net)

Monthly Graph

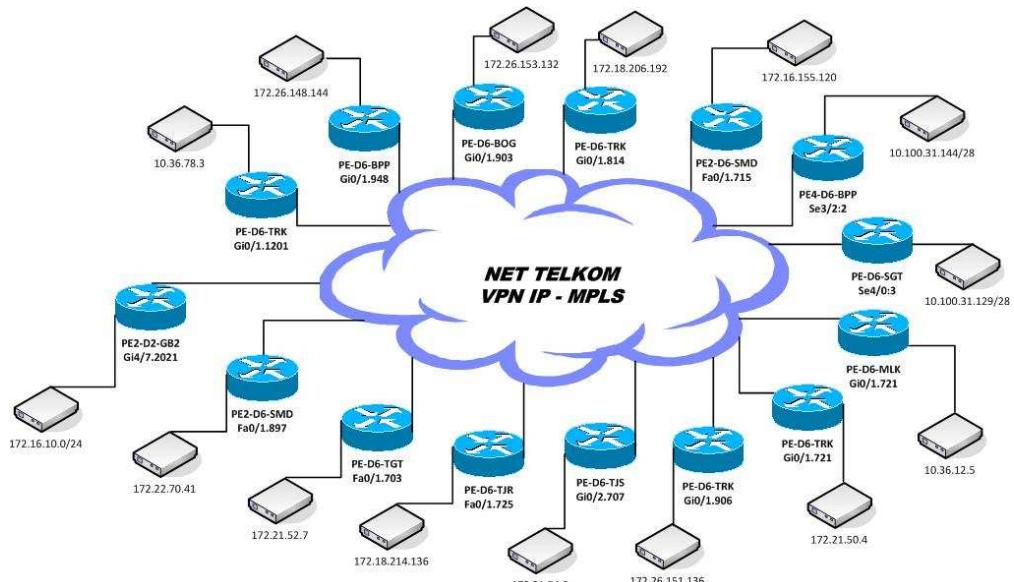


Gambar 8. Capture Traffic Back Haul VPN IP KPU Pusat dari tanggal 8 April 2009 s.d 8 Mei 2009
(Sumber: www.mrtg.telkom.net)

Dari MRTG dapat kita lihat bahwa *incoming* maupun *outcoming traffic* sudah cukup optimal terutama pada masa-masa perhitungan suara mulai dari tanggal 9 April 2009 sampai dengan 9 Mei 2009 diperoleh :

Tabel 4. Incoming dan Outcoming Traffic

| Traffic | Minimum | Maximum | Average |
|-----------|----------|-------------|------------|
| Incoming | 3,8 kbps | 3244,5 kbps | 509,3 kbps |
| Outcoming | 4,2 kbps | 3223,1 kbps | 544,1 kbps |



Gambar 9. Konfigurasi Link Standard Layanan VPN IP Pemilu 2009

Seperti telah dijelaskan sebelumnya bahwa jalur komunikasi yang digunakan adalah *VPN (Virtual Private Network)* dengan dukungan kecepatannya pun sangat tinggi untuk di sisi back haul KPU Pusat di Jakarta 30 Mbps. Hanya saja karena banyaknya data yang harus diupload dari masing-masing KPUD Kabupaten/Kota salah satu faktor lambatnya penerimaan data di server KPU Pusat. Idealnya memang untuk mengolah data KPU ini diperlukan minimal 30 server berkecepatan tinggi.

Proses pengolahan data perolehan suara yang terekam dalam formulir C1-IT yang telah diisi terlebih dahulu *scan* di KPUD Kabupaten/Kota, proses *scan* ini dilakukan secara manual oleh masing-masing operator IT Pemilu 2009 di masing-masing KPUD Kabupaten/Kota. Karena proses ini dilakukan secara manual, maka jelas memerlukan waktu pemrosesan, karena untuk formulir C1-IT ini berjumlah 8 lembar. Hasil dari scan formulir C1-IT secara langsung akan menghasilkan 8 buah citra, dan data citra inilah yang akan dibaca oleh (*Intelligent Character Recognition*) lalu dikonversi menjadi kode-kode huruf ASCII.

Sebelum file tersebut dikirim ke server KPU akan dilakukan beberapa tahapan, seperti verifikasi, pengecekan, dan sebagainya. Tahapan tersebut selain memerlukan tenaga IT yang baik, juga diperlukan komputer berkecepatan tinggi, memori besar, space yang besar serta jalur komunikasi yang baik, sangat direkomendasikan menggunakan jalur komunikasi serat optik. Tahapan atau proses inilah yang membuat lambatnya proses pengiriman data dari KPUD ke KPU Pusat.

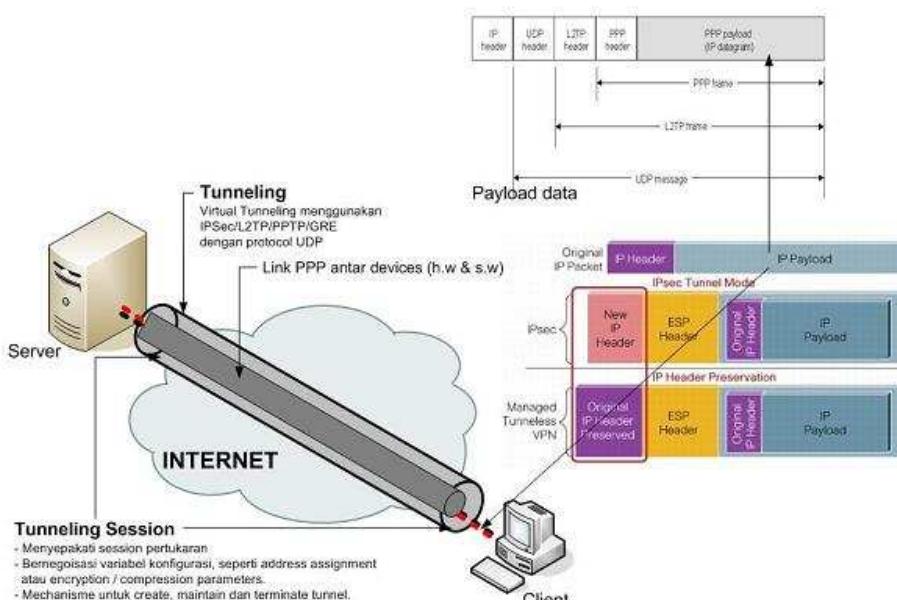
Apabila tidak terjadi kesalahan pada tahapan tersebut, hasilnya akan dikirim ke server KPU menggunakan jalur *VPN (Virtual Private Network)*. Penggunaan jalur ini memang secara teknologi jauh lebih aman, baik dari gangguan *spam*, *virus*, *phishing* dan sebagainya. Karena jalur ini berbeda dengan jalur internet pada umumnya. Setelah data tersebut sampai di server KPU, selanjutnya akan dilakukan beberapa proses, lalu apabila dinyatakan aman, data akan langsung diupload ke web server KPU dan hasilnya bisa dibaca melalui situs resmi KPU.

Dalam hal ini sebelum masuk ke web server KPU melalui *VPN (Virtual Private Network)* merupakan sebuah jaringan *private* yang menghubungkan satu *node* jaringan ke *node* jaringan lainnya dengan menggunakan jaringan internet. Data yang dilewatkan akan *diencapsulation* (dibungkus) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya.

Jaringan VPN dikoneksikan oleh ISP (*Internet Service Provider*) yakni Telkom melewati routernya (router PE) ke router-router lain dengan menggunakan jalur internet yang telah dienkripsi antara dua titik, dengan menggunakan *leased line* untuk hubungan jarak jauh dengan VPN, semestinya instansi dapat menghemat 20% sampai 40% dari biaya WAN.

Mengapa jaringan yang menggunakan VPN ini dianggap aman? Hal ini karena Sistem keamanan di VPN menggunakan beberapa lapisan, diantaranya:

1. Metode *Tunneling* (terowongan), membuat terowongan virtual di atas jaringan publik menggunakan protokol seperti *Point To Point (PPTP)*, *Layer 2 Tunneling Protocol (L2TP)*, *Generic Routing Encapsulation (GRE)* atau *IP Sec*. PPTP dan L2TP adalah layer 2 tunneling protocol. Keduanya melakukan pembungkusan payload pada frame *Point to Point Protocol (PPP)* untuk dilewatkan pada jaringan. IP Sec berada di layer 3 yang menggunakan packet, yang akan melakukan pembungkusan IP header sebelum dikirim ke jaringan.



Gambar 10. Skema Tunneling dan Encapsulation Pada Jaringan VPN

2. Metode Enkripsi untuk *Encapsulation* (membungkus) paket data yang lewat di dalam tunneling, data yang dilewatkan pada pembungkusan tersebut, terlebih dahulu data disini akan diubah dengan metode algoritma kriptography tertentu seperti DES, 3DES, atau AES.
3. Metode Otentikasi User, karena banyak user yang akan mengakses biasanya digunakan beberapa metode otentikasi user seperti *Remote Access Dial In User Services (RADIUS)* dan *Digital Certificates*.
4. Integritas Data, paket data yang dilewatkan di jaringan publik perlu penjaminan integritas data/kepercayaan data apakah terjadi perubahan atau tidak. Metode VPN menggunakan HMA C-MD5 atau HMA C-SHA1 untuk menjadi paket tidak dirubah pada saat pengiriman.

Jika diamati lingkup layanan IP MPLS yang diberikan oleh provider dalam hal ini Telkom dibatasi namun masih bersifat fleksibel, artinya lingkup Telkom dapat ditambah dengan lingkup lain apabila instansi dalam hal ini KPU selaku *customer* menginginkannya. Penambahan lingkup dan model bisnis yang terkait dengan hal itu disepakati dalam tahapan desain implementasi layanan. Telkom selaku penyedia jaringan dari *node (cloud)* terdekat sampai dengan modem di sisi pelanggan, artinya bahwa modem yang berada di *customer* termasuk dalam lingkup penyediaan Telkom (*manageable by provider*). Sedangkan di sisi *customer* menyediakan perangkat *router*, serta perangkat-perangkat security firewall dan LAN (*Local Area Network*).

Multiservices Platform yang mungkin dikembangkan adalah layanan voice, video dan grafis disamping layanan data. Dengan demikian berbagai aplikasi bisnis dengan jaminan CoS yang sesuai dapat dijalankan pada IP MPLS, seperti : video conference, VoIP, aplikasi ERP, CRM dan lain-lain. Dengan sifat scalability dan kelebihannya maka layanan VPN IP MPLS dapat dimulai dari skala jaringan yang kecil dan terbatas dapat dikembangkan secara tepat, mudah dan praktis meliputi bandwidth dan konfigurasinya.

Dengan tingkat efisiensi penggunaan bandwidth dan customized CoS sesuai jenis trafik, biaya yang dikeluarkan sebagai harga sewa ke provider IP MPLS semestinya dapat ditekan lebih rendah dibandingkan dengan jaringan lain seperti *clear-leased channel* atau *frame relay*.

5. KESIMPULAN

Dari penjelasan di atas dapat disimpulkan bahwa:

- 1) Penggunaan teknologi komunikasi data berbasis VPN IP MPLS untuk Pemilu 2009, untuk proses awal seperti scanning Formulir C1-IT, pengiriman data dari KUPD ke KPU Pusat sangat tepat dan sangat aman karena jalur yang digunakan merupakan jalur VPN. Sehingga gangguan spam dan hacker pada tahap ini tidak akan terjadi. Namun perlu diantisipasi ketika data tersebut diproses dan diupload ke Web Sever KPU bisa saja pembobolan dari hacker terjadi.
- 2) Pemanfaatan fitur layanan pada VPN IP MPLS khususnya layanan data untuk Pemilu 2009 telah dipergunakan secara optimal dari yang disediakan. Perlu dikembangkan fitur-fitur yang lain seperti video conference, VoIP dan aplikasi lain untuk lebih memaksimalkan fitur-fitur yang bisa dilayani oleh jaringan VPN IP MPLS.
- 3) Teknologi komunikasi data VPN IP MPLS yang diterapkan belum didukung oleh *skill* operator IT KPU/KPUD di lokasi karena masih sering terjadi anomali perangkat seperti tidak bisa mengoperasikan *scanner* dan tidak bisa menggunakan aplikasi ICR, hal ini juga ditemukan oleh peneliti.
- 4) Kelambatan proses perhitungan suara juga dapat disebabkan kurangnya perangkat pendukung seperti server dan lainnya, karena idealnya server yang perlu disediakan sebanyak 30 buah.

6. DAFTAR PUSTAKA

- , "Bab VI Studi Literature." <http://js.unikom.ac.id/rb/bab6.html>. Diakses tanggal 23 Maret 2009
- , "Studi Lapangan." http://www.infosripsi.com/component?option=com_glossary&Itemid,62/....,Studilapangan/. Diakses tanggal 23 Maret 2009
- Darmawan, Indra. 2009. Melongok Sistem TI Pemilu 2009. http://teknologi.vivanews.com/news/read/48053-melongok_sistem_ti_pemilu_2009. Diakes tanggal 20 April 2009.
- DetikNet. 2009. Telkom Menang Tender Jaringan Pemilu 2009. <http://fema.ipb.ac.id/bem/?p=211>. Diakses tanggal 24 Maret 2009
- Kana, Willem A. 2005. *Keamanan dan Layanan VPN Dalam Arsitektur Jaringan MPLS*. Bandung: Institut Teknologi Bandung.
- Odom, Wendell. 2005. *Computer Networking First-Step*. Yogyakarta: Penerbit Andi.
- Stiawan, Deris. *Membangun Interkoneksi VPN dengan solusi Hardware-Based dan Jaringan IIX*. Jurusan Sistem Komputer, FASILKOM UNSRI.
- SubDiv Corporate Customer Care. 2005. *Pedoman Kegiatan Customer Handling di Lingkungan Unit Kerja Corporate Customer Care Center (C4)*. Jakarta: Divisi Enterprise Service PT. Telkom Indonesia.

- Suratmo, Yayat. 2008. "Jadwal Tahapan Pemilu 2009."
<http://www.kabarinetnews.com/article.cfm?articleID=32301>. Diakses tanggal 4 April 2009.
- Tutang MM, Pranata Komputer Madya – LIPI. 2009. "Lambatnya server KPU."
http://teknologi.vivanews.com/news/read/48053-melongok_sistem_ti_pemilu_2009. Diakses tanggal 1 Mei 2009
- Yusup, Pawit M. "Bab VI Studi Wawancara." <http://www.scribd.com/doc/6067744/Studi-Wawancara>. Diakses tanggal 25 Maret 2009.