

JARINGAN PENGAMATAN TERPADU SAINS ATMOSFER MENGUNAKAN VPN IP

Rizal Suryana¹, Wendi Harjupa¹, Ori Novanda²

¹LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL (LAPAN)
Jl. DR DJUNDJUNAN NO 133 BANDUNG

rizal@bdg.lapan.go.id

wendi@bdg.lapan.go.id

²UNIVERSITAS SUMATRA UTARA
Jl. Dr. Mansyur no 9 Medan Sumatra Utara

Ori.novanda@gmail.com

Abstract

Lapan Bandung has six observation station located on the island of Java, Sumatra, Kalimantan and Papua, where the atmospheric observation doing on observatory station. The data observation were not sent directly to the data center Lapan Bandung, this is due to a network that is not integrated in the observatory station with Lapan Bandung. The process of sending data from the observatory station to Lapan Bandung and a data management necessary infrastructure and supporting technologies. Satellite is a communications technology that can connect between one node to the central node and can reach the entire territory of a country. Data transmission via a public network satellite communications or the internet network needed a privacy / data security, for security a data in transmission process will use a network of Virtual Private Network (VPN) as a backbone network between Lapan Bandung as a data center with all the observatory stations as a branch. Atmospheric observation network for the all observation station in an integrated can be formed using an VPN IP network through communication satellites and a data observation sent to the data center automatically either realtime or near relatime.

Keyword : Data Center, Computer Network Integrated, VPN IP

Abstrak

LAPAN Bandung memiliki 6 stasiun pengamatan dirgantara yang berada di pulau Jawa, Sumatra, Kalimantan dan Papua, dimana pengamatan atmosfer dilakukan pada stasiun pengamat dirgantara tersebut. Data hasil pengamatan tidak langsung dikirim ke data center LAPAN Bandung, hal ini disebabkan belum terintegrasinya jaringan yang berada di masing-masing stasiun pengamat dirgantara dengan LAPAN Bandung. Proses pengiriman data dari stasiun pengamat dirgantara ke LAPAN Bandung dan manajemen data dibutuhkan suatu sarana dan teknologi pendukung. Satelit merupakan sebuah teknologi komunikasi yang dapat menghubungkan antara satu node dengan pusat node dan dapat menjangkau seluruh wilayah suatu negara. Pengiriman data melalui jaringan publik komunikasi satelit atau jaringan internet diperlukan sebuah privasi/keamanan data, untuk menjaga keamanan data dalam proses pengiriman menggunakan jaringan Virtual Private Network (VPN) sebagai tulang punggung jaringan antara LAPAN Bandung sebagai pusat dengan seluruh stasiun pengamat dirgantara sebagai cabang. Jaringan pengamatan atmosfer untuk seluruh stasiun pengamatan dirgantara secara terpadu dapat dibentuk dengan menggunakan jaringan VPN IP melalui komunikasi satelit dan data hasil pengamatan terkirim ke data center secara otomatis baik realtime maupun near relatime.

Kata Kunci : Data Center, Jaringan Komputer, VPN IP

1. PENDAHULUAN

Stasiun pengamat dirgantara Tanjungsari, Pameungpeuk, Watukosek, Biak, Pontianak dan Kototabang merupakan lokasi pengamatan yang selama ini digunakan. Pada masing – masing lokasi pengamatan terdapat alat pengamatan yang berbeda-beda

diantaranya : Automatic Weather Station (AWS), Equatorial Atmosphere Radar (EAR), X-Band radar, Radiometer, RASS, Desdrometer, ORG, Microrain Radar, MicroBarographs, Light Detection and Ranging (LIDAR) dan Ozone Monitor. Data hasil pengamatan dikirim ke LAPAN Bandung dengan cara semua data hasil pengamatan di backup kedalam CD/DVD kemudian dikirimkan melalui Jasa pengiriman barang, atau data dikirim melalui email secara periodik ke peneliti yang bersangkutan. Metode seperti ini dapat dilakukan dalam interval waktu 1 jam atau sebulan sekali, pengiriman data melalui email dapat mempercepat pengiriman namun kapasitas pengiriman data hanya mampu sebesar 4 Mb dalam satu kali pengiriman dan keberadaan data menjadi tidak tertata dengan baik. Pengiriman data hasil pengamatan dapat dilakukan dalam jumlah besar dengan cara data di backup ke dalam semua media CD/DVD dan di kirimkan melalui jasa pengiriman barang, cara seperti ini data akan sampai ke LAPAN Bandung paling cepat 24 jam dan dipengaruhi oleh faktor tingkat kerajinan operator pengumpul data.

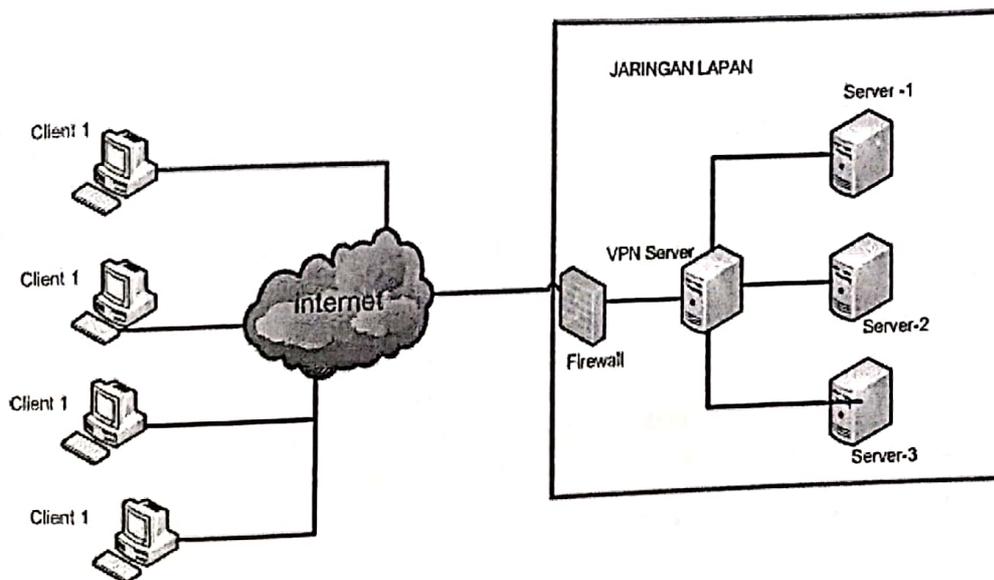
Dalam melakukan koneksi antara satu jaringan dengan jaringan yang lain dapat menggunakan media kabel dan gelombang radio. Jenis media kabel yang digunakan dalam pembuatan jaringan komputer adalah jenis kabel UTP, dengan menggunakan kabel UTP maksimum jarak yang bisa dijangkau yaitu 100 meter (Jaka fahrial, 2003) sedangkan jarak terdekat antara stasiun pengamat dirgantara dengan kantor penyedia jasa layanan (ISP) yaitu 35 Km. Kabel serat optik merupakan sebuah media fisik yang dapat digunakan sebagai saluran komunikasi data dan suara serta memiliki bandwidth lebih sebesar 100 Mbps. Jarak yang maksimum yang dapat di tempuh yaitu 2 Km (Jaka fahrial, 2003), sebenarnya jarak yang dapat dicapai dengan kabel serat optik sampai ratusan kilo meter yaitu dengan cara menambahkan penguatan pada setiap ujung kabel serat optik. Permasalahan dengan menggunakan kabel fiber optik adalah biaya instalasi dan perbaikan mahal, karena kabel serat optik dalam pemasangannya dilakukan dalam tanah. Pembangunan jaringan komputer dapat dilakukan dengan menggunakan gelombang radio seperti Wifi, bluetooth dan Wimax. Proses mengkoneksikan antara satu jaringan dengan jaringan yang dengan menggunakan media gelombang radio, kondisi geografis sangat mempengaruhi keberhasilan komunikasi. Jika kondisi geografis terdapat banyak bukit, gunung dan gedung-gedung bertingkat akan menjadikan suatu kendala, karena sifat dari gelombang radio untuk frekuensi tinggi tidak dapat memantul jika terhalang suatu bangunan atau bukit.

Proses pengiriman data hasil pengamatan dari masing-masing stasiun pengamat dirgantara dapat dilakukan melalui jaringan publik seperti internet, data yang dikirimkan ke server LAPAN bandung dapat secara realtime atau near realtim dalam jumlah yang besar. Masalah keamanan data menjadi faktor yang sangat penting, karena internet merupakan jaringan global yang dapat menghubungkan setiap jaringan komputer diseluruh dunia. Kecepatan pengiriman data akan sangat pengaruhi oleh jumlah pengguna internet dalam satu jaringan, misalkan stasiun pengamat dirgantara pontianak memiliki jumlah komputer 10 unit dan terkoneksi dengan internet, pada saat jam kerja semua komputer menggunakan fasilitas internet maka pada saat ini besarnya bandwidth akan dibagi dengan jumlah komputer. Teknologi media komunikasi antara jaringan stasiun pengamat dirgantara dengan LAPAN Bandung menggunakan media komunikasi radio dengan melalui VSAT dan Wimax. VSAT digunakan pada stasiun pengamat dirgantara Tanjungsari, Pameungpeuk dan Kototabang, penggunaan VSAT pada ketiga stasiun pengamat dirgantara disebabkan kondisi geografis yang berada diantara bukit-bukit dan gunung. Sedangkan untuk stasiun pengamat dirgantara pontianak menggunakan media komunikasi radio menggunakan Wimax, karena jarak dan kondisi geografis yang tidak terhalang oleh gedung tinggi, bukit-bukit dan gunung. Sebagai solusi untuk mengatasi

masalah keamanan dan pengaruh bandwidth maka pengiriman data dari masing-masing stasiun pengamat dirantara dilakukan menggunakan Virtual Private Network (VPN).

2. TINJAUAN PUSTAKA

Yang dimaksud dengan Virtual Private Network (VPN) adalah suatu jaringan private yang mempergunakan sarana jaringan komunikasi publik (dalam hal ini Internet) dengan memakai *tunneling protocol* dan prosedur pengamanan (Tri Wahyu Nugroho, 2006). Dengan memakai jaringan publik yang ada, dalam hal ini Internet, maka biaya pengembangan yang dikeluarkan akan jauh relatif lebih murah daripada harus membangun sebuah jaringan internasional tertutup sendiri. Namun pemakaian Internet sebagai sarana jaringan publik juga mengandung resiko, karena Internet terbuka untuk umum, maka masalah kerahasiaan dan autentifikasi atas data yang dikirim pun juga terbuka. Oleh karenanya VPN menjaminkannya dengan penerapan enkripsi data. Sebelum dikirimkan, terlebih dahulu data akan dienkripsikan untuk mengurangi resiko pembacaan dan pembajakan data di jalan oleh pihak yang tidak terkait. Setelah sampai ke alamat tujuan, maka data tersebut akan di-deskripsikan ulang sehingga bentuk informasi dapat kembali menjadi seperti sedia kala. Selain memakai metode pengamanan enkripsi-deskripsi, VPN masih memakai kriptografi lainnya untuk mendukung pengamanan data.



Gambar 2.1. Jaringan VPN

VPN merupakan solusi koneksi private melalui jaringan publik. Dengan VPN maka kita dapat membuat jaringan di dalam jaringan atau biasa disebut tunnel. Solusi VPN ada beberapa macam. Antara lain:

1. IPSEC, solusi VPN via IP Secure Protocol. Solusi yang sudah distandarisasi tapi paling susah dikonfigurasi. Tingkat keamanan yang cukup baik namun dalam implementasinya cukup rumit. Aplikasi yang digunakan yang berbasis open source yaitu Open/Free Swan.
2. PPPT, solusi VPN versi awal. Merupakan solusi VPN dengan feature standar dimana jaringan dibangun dengan point to point seperti halnya anda melakukan dial up pada internet dirumah. Pada saat dial up ke provider internet ada maka akan

dibangun point to point tunnel melalui jaringan telepon. Aplikasi OpenSource yang menggunakan PPPT adalah PopTop.

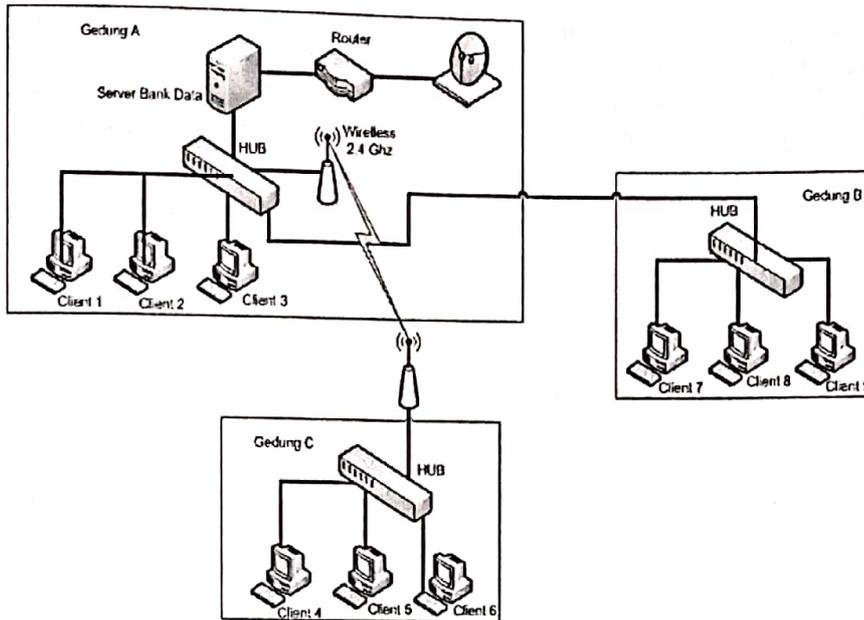
3. VPN with SSL, merupakan solusi VPN dengan menerapkan protocol Secure Socket Layer(SSL) pada enkripsi jaringan tunnel yang dibuat. Solusi ini diawali dengan aplikasi OpenVPN.

Fungsi VPN ada banyak. Beberapa diantaranya yaitu:

- e. Menghubungkan kantor-kantor cabang melalui jaringan public. Dengan VPN maka perusahaan tidak perlu membangun jaringan sendiri. Cukup terhubung dengan jaringan public contohnya internet. Saat ini hampir semua kantor perusahaan pasti memiliki akses internet. Dengan demikian bisa dihemat anggaran koneksi untuk ke cabang-cabang.
- f. Mobile working, dengan VPN maka karyawan dapat terhubung langsung dengan jaringan kantor secara private. Maka karyawan dapat melakukan pekerjaan yang bisa dilakukan dari depan komputer tanpa harus berada di kantor. Hal ini menjadi solusi virtual office di jaman mobilitas tinggi seperti sekarang ini.
- g. Securing your network. Saat ini beberapa vendor seperti telkom memberikan solusi VPN juga untuk perusahaan-perusahaan. Namun solusi ini masih kurang aman. Karena untuk terhubung tidak memerlukan autentikasi. Sehingga bila ada pengguna mengetahui setingan VPN perusahaan tersebut maka dia dapat terhubung ke jaringan perusahaan tapi harus login. Contohnya pada telkomsel VPN hanya dengan mengganti nama APN pada setingan network maka dia dapat langsung terhubung dengan jaringan dengan nama APN tersebut. Dengan memasang VPN lagi di jaringan VPN semi publik tersebut maka jaringan akan lebih aman karena sebelum masuk ke jaringan kantor maka user harus membuat tunnel dulu dan login ke VPN server baru bisa terhubung dengan jaringan kantor.
- h. Mengamankan jaringan wireless. Jaringan wireless merupakan jaringan publik yang bisa diakses oleh siapa saja yang berada dijangkauan wireless tersebut. Walaupun wireless juga memiliki pengaman seperti WEP, WPA, WPA2 namun jaringan wireless masih saja bisa ditembus. Dengan menggunakan VPN maka user yang terhubung ke wireless harus membuat tunnel dulu dengan login ke VPN server baru bisa menggunakan resource jaringan seperti akses internet dan sebagainya.

3. HASIL DAN PEMBAHASAN

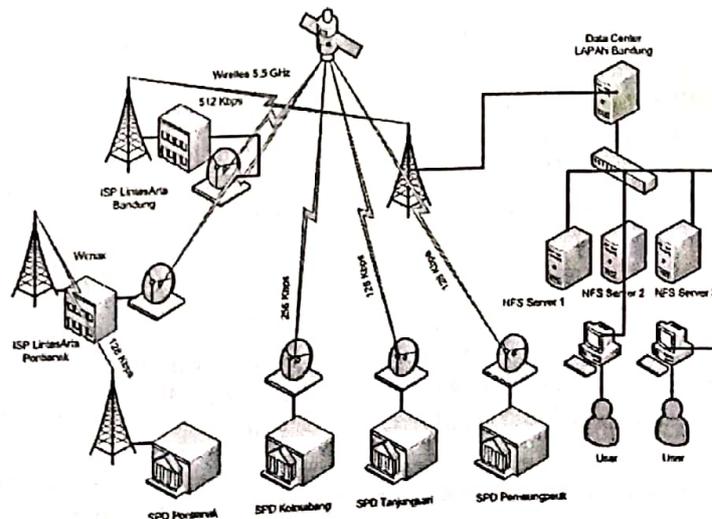
Jaringan lokal untuk setiap stasiun pengamat dirantara menggunakan topologi pohon (tree topologi), seperti ditunjukkan dalam Gambar 3.1. Penggunaan topologi pohon digunakan karena komputer tersebar disetiap ruangan yang berbeda, media fisik yang digunakan adalah menggunakan kabel UTP cat 6 dengan kecepatan 1 Gbps, media fisik digunakan untuk jarak antara gedung yang tidak lebih dari 120 meter sedangkan untuk jarak yang lebih dari 120 meter menggunakan media gelombang radio dengan frekuensi 2,4 Ghz.



Gambar 3.1. Jaringan Lokal Stasiun Pengamat Dirgantara

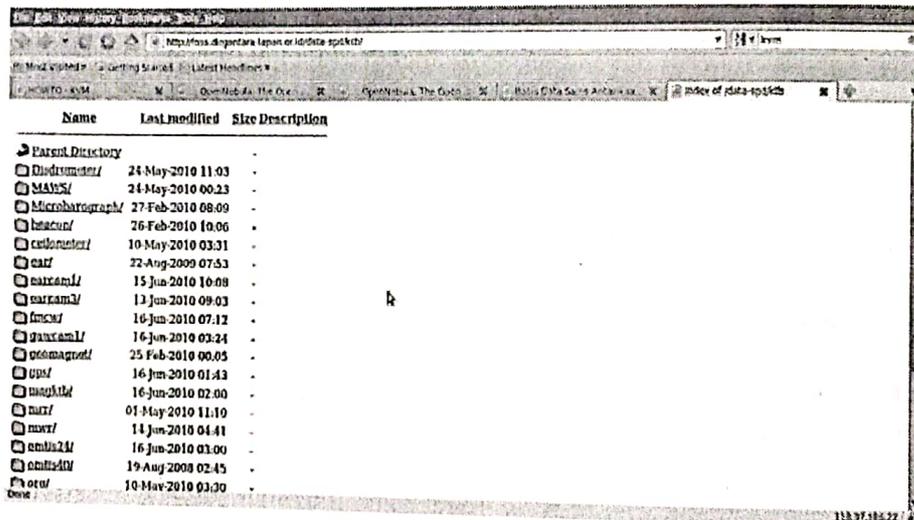
Keuntungan pembangunan jaringan komputer menggunakan topologi pohon adalah Pengembangan jaringan kedepan lebih mudah, dengan adanya kabel tersendiri untuk setiap cleint ke server, maka bandwidth atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan kinerja jaringan secara keseluruhan, bila terdapat gangguan di suatu jalur kabel maka gangguan hanya akan terjadi dalam komunikasi antara cleint yang bersangkutan dengan server dan jaringan keseluruhan tidak mengalami gangguan.

Koneksi antara stasiun pengamat dirgantara dengan LAPAN Bandung untuk SPD Tanjungsari, Pemungpeuk dan Kototabang menggunakan VSAT (Gambar 3.2), karena kondisi geografis ketiga SPD tersebut berada diluar jangkauan wireless Provider LintasArta. Sedangkan untuk SPD Pontianak menggunakan Wimax. Perbedaan koneksi VSAT dengan wimax adalah delay time (waktu tunda), VSAT memiliki delay time 600ms sedangkan Wimax 1ms, Perbedaan ini akan mempengaruhi kecepatan transfer data.



Gambar 3.2. Internetworking Jaringan Pengamatan Sains Atmosfer

Interkoneksi antara jaringan komputer stasiun pengamat dirgantara dengan LAPAN Bandung menggunakan VPN IP yang berjalan di atas jaringan publik komunikasi satelit. Dalam pembangunan VPN untuk jaringan pengamatan terdapat sains atmosfer memakai teknologi Mult Protocol Label Switching (MPLS) menerapkan full mesh TE (Traffic Engineering) Tunnels, menciptakan logika mesh, walaupun topologi fisik tidak full mesh. Pada situasi seperti ini, kondisi jaringan telah memperoleh tambahan 40% - 50% ketersediaan bandwidth di jaringan. Keuntungannya penggunaan jaringan secara optimal, yang berperan penting pada penurunan capital expenses (Mudji Basuki, 2007). Sehingga dapat meningkatkan kualitas pengiriman paket data dalam jaringan berkecepatan tinggi. Cara kerja MPLS adalah dengan menyelipkan *label* di antara *headerlayer2* dan *layer3* pada paket yang diteruskan. Label dihasilkan oleh *Label-Switching Router* dimana bertindak sebagai penghubung jaringan MPLS dengan jaringan luar. *Label* berisi informasi tujuan *node* selanjutnya kemana paket harus dikirim. Kemudian paket diteruskan ke *node* berikutnya, di *node* ini label paket akan dilepas dan diberi label yang baru yang berisi tujuan berikutnya. Paket-paket diteruskan dalam path yang disebut *Label Switching Path (LSP)* (Kuncoro Wastuwibowo, 2003).



Gambar 3.3 Data Hasil Pengiriman dari Stasiun Pengamat Dirgantara.

Integrasi Jaringan komputer stasiun pengamat dirgantara dengan LAPAN Bandung, memudahkan pengguna dalam melakukan pengambilan data hasil pengamatan, seperti ditunjukkan dalam Gambar 3.3. Data hasil pengamatan di download dari masing – masing komputer peralatan oleh server bank data SPD dengan sistem sinkronisasi. Server data server bank data SPD, kemudian data center akan menyimpan data berdasarkan nama stasiun pengamat dirgantara kedalam *Network files System (NFS)* server. Data hasil pengamatan akan menempati satu NFS server, dimana NFS server memiliki kapasitas penyimpanan data sebesar 1,5 TB dan dapat di tingkatkan menjadi 4 TB. Server data center akan memetakan setiap data yang berada pada NFS server yang berfungsi untuk memudahkan pengguna dalam melakukan pengambilan data. Pengguna dapat mengambil data hasil pengamatan dari Data Center LAPAN Bandung pada alamat <http://foss.dirgantara-lapan.or.id/lafica> yang setiap saat selalu terupdate atau mengambil secara langsung dari komputer peralatan dari masing-masing stasiun pengamat dirgantara.

4. KESIMPULAN

Stasiun pengamat dirgantara terintegrasi kedalam satu jaringan menggunakan VPN IP dengan alokasi bandwidth untuk stasiun pengamat dirgantara Kototabang 256 Kbps, stasiun pengamat dirgantara Tanjungsari 128 Kbps, stasiun pengamat dirgantara Pontianak 128 Kbps dan stasiun pengamat dirgantara Pameungpeuk 128 Kbps. Walaupun bandwidth yang tersedia relatif kecil tapi pengiriman data dengan jumlah besar dapat berjalan dengan baik, hal ini disebabkan karena menggunakan teknologi MPLS. Tersedianya jaringan VPN antara stasiun pengamat dirgantara dengan LAPAN Bandung sehingga pengambilan data dari masing-masing komputer pengamatan dilakukan secara otomatis tanpa dilakukan oleh operator dengan sistem sinkronisasi. Proses pengiriman data menjadi lebih cepat sampai kepada peneliti baik secara real time ataupun near realtime, peralatan pengamat dapat termonitoring setiap saat oleh para peneliti atau teknisi LAPAN Bandung. Data hasil pengamatan dikelola pada satu pusat data center sehingga manajemen data menjadi baik.

UCAPAN TERIMAKASIH

Penulis mengucapkan banyak terimakasih kepada Ka. Instalmentan yang telah memberikan kepercayaan sehingga proyek penelitian dapat berjalan dan berhasil, Kepada panitia seminar sains atmosfer yang telah menerima makalah ini dan serta semua anggota team Jaringan LAPAN Bandung Pak Syahril, Ibu Elly, Ibu Mariam, Alhadi saputra dan Yoestiana yang telah banyak membantu membangun jaringan integrasi stasiun pengamat dirgantara LAPAN Bandung.

DAFTAR RUJUKAN

- Charlie Scott, Paul Wolfe, Mike Erwin., January 1999, Virtual Private Network, O'Reilly Second Edition.
- Kuncoro Wastuwibowo., November 2003, Jaringan MPLS, Whitepaper Telkom.
- Muji Basuki., Februari 2008, Positioning MPLS, Artikel Ilmu Komputer.
- Tri Wahyu Nugroho., 2006, Penggunaan Virtual Private Network (VPN), Divkom ITB.
- Winarno Sugeng., Agustus 2006, Jaringan Komputer Dengan TCP/IP, Informatika.