BAB III
PEMBAHASAN

3.1 Waktu dan Tempat

Tempat pelasanaan kerja praktek di dinas komunikasi dan informatika provinsi jawa barat. Jl. Tamansari no.55 Bandung Tlp. (022)-2502898 Fax. 022-2511505. Waktu pelaksanaan kerja praktek selama satu bulan dimulai tanggal 19 juni 2010 sampai 15 agustus 2010.

3.2 Lokasi Proyek Jaringan

Pada implementasi ini akan dibangun jaringan antara Dinas komnikasi dan Informatika (DISKOMINFO) dengan Satuan Organisasi Perangkat Daerah (SOPD) di Jawa Barat yang mencangkup :

1. Dinas Komunikasi dan Informatika

   Alamat Jl. Tamansari 55 Bandung Tlp. (022)-2502898 Fax. 022-2511505

   email: info@jabarprov.go.id http://www.diskominfo.jabarprov.go.id/

2. Dinas Kesehatan

   Alamat Jl.Pasteur no. 25 (022) 4232292

   Website http://diskes.jabarprov.go.id

3. Dinas Pendapatan

   Alamat Jl. Soekarno Hatta no. 528 Bandung, (022) 7566197

   Website http://dispenda.jabarprov.go.id

4. Dinas Pendidikan

   Alamat Jl. Dr. Radjiman no. 6 Bandung

   Website http://disdik.jabarprov.go.id

5. Dinas Peternakan

   Alamat Jl. Ir. H. Juanda no. 358 Bandung, (022) 2501151

   Website http://disnak.jabarprov.go.id

6. Dinas Kehutanan

   Alamat Jl. Soekarno-Hatta 751 Bandung, (022)7304029

   Website http://dishut.jabarprov.go.id

7. Dinas Perkebunan

   Alamat Jl. Surapati no. 67 Bandung, (022) 2038966

   Website http://disbun.jabarprov.go.id

8. Dinas Perhubungan

   Alamat Jl. Sukabumi No. 1 Bandung, (022) 7272258

   Website www.dishub.jabarprov.go.id/

9. Dinas bina marga
   Alamat : Jl. Asia Afrika no. 79 Bandung No. Telp. : 022-4231634
   Website http://disbinmar.jabarprov.go.id/

10. Dinas Energi dan Sumber Daya Mineral

    Alamat Jl. Soekarno Hatta 576 Bandung, (022) 7562048

    Website http://esdm.jabarprov.go.id

Lokasi dinas-dinas berada di dalam satu wilayah seperti dinas DISKOMINFO yang berada di wilayah kota Bandung, Begitu juga dinas-dinas SOPD yang berada tersebar di daerah-daerah Di wilayah Jawa Barat khususnya di kota bandung, Dari semua dinas tersebut akan dibangun jaringan yang dapat saling berkomunikasi satu dengan yang lainnya Untuk menunjang segala kebutuhan informasi dan komunikasi yang sangat baik. Untuk itu diperlukan peninjauan secara menyeluruh.

3.3 Aktifitas Yang Dikerjakan

Adapun aktifitas yang di kerjakan pada saat pembangunan jaringan ini di laksanakan diantaranya :

3.3.1 Pengendalian Jadwal

Kami telah memperoleh beberapa strategi atau cara untuk mengantisipasi adanya penyimpangan atau perubahan dalam penjadwalan pelaksanaan proyek ini yang biasanya terjadi di lapangan, yaitu antara lain :

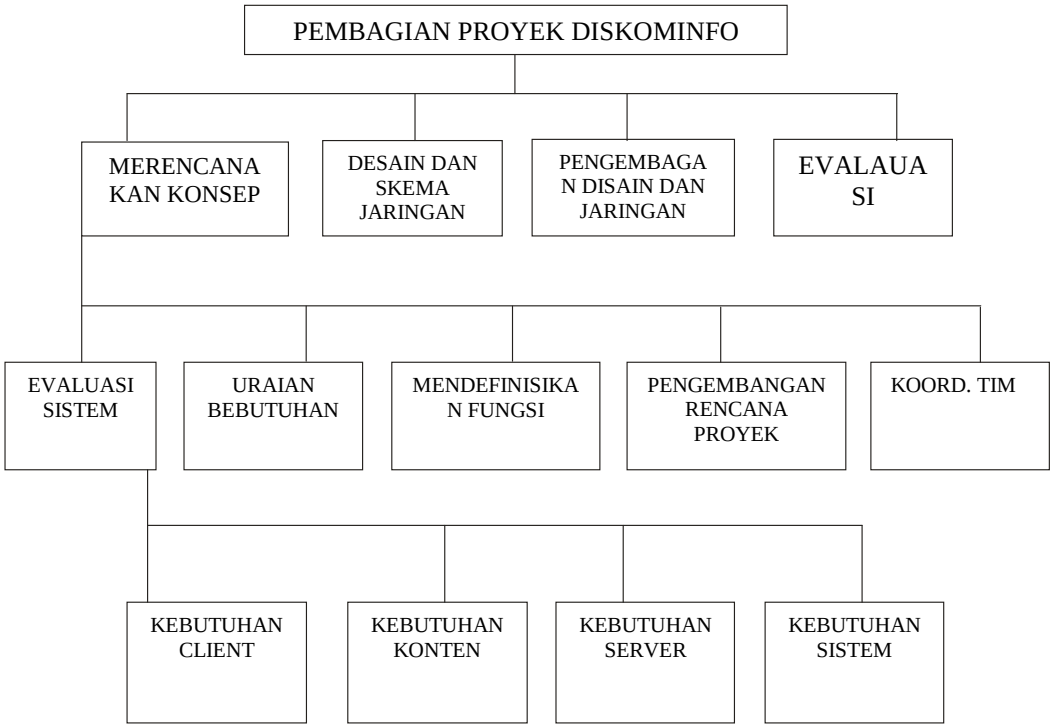
a. Meningkatkan kemampuan dalam merespon perubahan yang mungkin terjadi pada penjadwalan aktibitas pada proyek ini.
b. Melakukan penjadwalan ulang atas semua aktifitas -aktifitas yang telah dijdwalkan sebelumnya,
c. Mengusahakan penjadwalan proyek agar tetap akurat dan selesai tepat waktu dengan cara memberi pendidikan pada anggota tim proyek manjadi sumber daya yabih kompeten dan disiplin.

Awal dari proyek pembagunan jaringan antar DISKOMINFO dengan SOPD ini adalah menggunakan MPLS Network yang tahap perencanaan awal, seperti :

a. Merencakan konsep dari proyek yang akan dibuat ini
b. Merencanakan dengan jelas tujuan dari proyek ini
c. Merencanakan pembentukan dan tim pelaksana proyek,
d. Melakukan peninjauan lokasi yang telah ditentukan untuk dijadikan sasaran proyek. dan juga sebagai tempat untuk mendistribusikan koneksi internet keseluruhan user di DISKOMINFO dan SOPD.
e. Merencanakan ketersediaan sarana prasarana berupa barang atau jasa serta penggunaan sumber daya baik materi, manusia, dan biaya serta waktu.

Setelah merencanakan dan mendefinisikan pekerjaan atau aktifitas yang dibutuhkan dalam pembangunan proyek jaringan antara DISKOMINFO dengan SOPD di lingkungan provinsi jawa barat ini, langkah berikutnya adalah memilah-milah setiap rencana aktifitas menjadi suatu aktifitas atau kegiatan yang lebih dapat dikelola lagi, setelah itu kami akan bisa menyusun beberapa urutan aktifitas tersebut.

Tabel 3.1 Skema Proyek

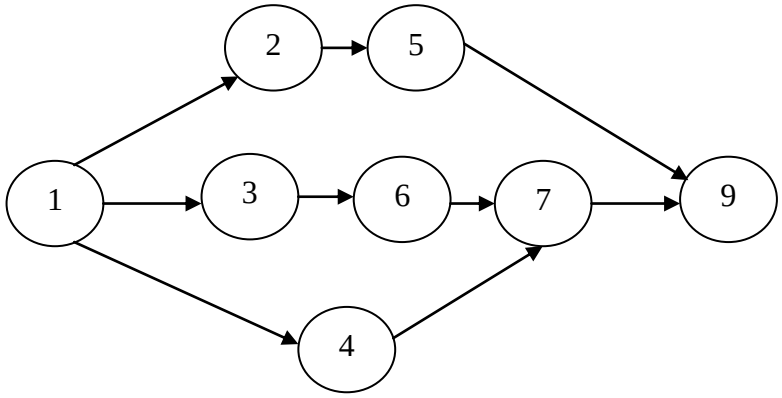


Setiap aktiftas kegiatan memiliki hubungan dan saling ketergantungan antar aktifitas. Ketergantungan inilah yang nantinya akan memudahkan tim proyek dalam menyusun urutan pekerjaan pada proyek yang akhirnya diwujudkan dalam betuk penjadwalan proyek.

Tabel 3.2 Aktivitas Proyek

NO	PEKERJAAN	KODE AKTIFITAS
1	analisis kebutuhan software	A
2	analisis kebutuhan hardware	B
3	desain skema	C
5	pengadaan dan instasali	D

5	survey / tinjauan	E
6	persiapan pelatiahan bagi client / pegawai	F
7	pengadaan	G
8	instalasi hardware	H
9	implementasi	I



Gambar 3.1 Alur Aktivitas Proyek

3.4 SDM (Sumber Daya Manusia)

Sumber daya manusia atau biasa disingkat menjadi SDM yaitu potensi yang terkandung dalam diri manusia untuk mewujudkan perannya sebagai makhluk sosial yang adaptif dan transformatif yang mampu mengelola dirinya sendiri serta seluruh potensi yang terkandung di lingkunganya serta tugas dia dalam mengerjakan sesuatu untuk menuju tercapainya kesejahteraan kehidupan dalam tatanan yang seimbang dan berkelanjutan baik bagi yang di kerjakan maupun bagi dirinya sendiri. Adapun sumber daya yang akan di butuhkan adalah :

3.4.1 Sumber Daya Manusia

3.4.1.1 Sumber Daya Manusia Institusi

Berdasarkan aktifitas pekerjaan dalam proyek ini diperlukan beberapa tenaga ahli di bidangnya dan berkompeten. Berdasarkan perencanaan jaringan yang ada, maka dinas harus menyiapkan sumbe daya manusia yang akan menjalankan monitoring dan operasional jaringan yang terlah terbangun, agar infrastruktur yang telah dibuat dapat berjalan optimal maka dibutuhkan.

1. 1 *Manager IT & Network*.
2. 4 Staff Ahli di Dinas pusat dan SOPD Masing-masing.
3. 1 Staff IT di tiap cabang SOPD.
4. Serta staff-staff yang membawahi bagian TI

Untuk penanganan jaringan yang telah di bangun maka sumber daya manusia yang telah di tentukan berperan berdasarkan fungsinya masing-masing.

3.4.1.2 Sumber Daya Manusia Pekerja

Dalam pembangunan ini akan membutuhkan tenaga ahli dalam pelaksanaanya, ada pun sumber daya yang di butuhkan yaitu :

1. Tenaga kerja di bidang analis jaringan dan pemetaan
2. Tenaga kerja di bidang distribusi perangkat yang dibutuhkan
3. Tenaga kerja di bidang penerapan dan implementasi
4. Tenaga kerja di bidang pengujian

3.4.2 Sumber Daya Materiil

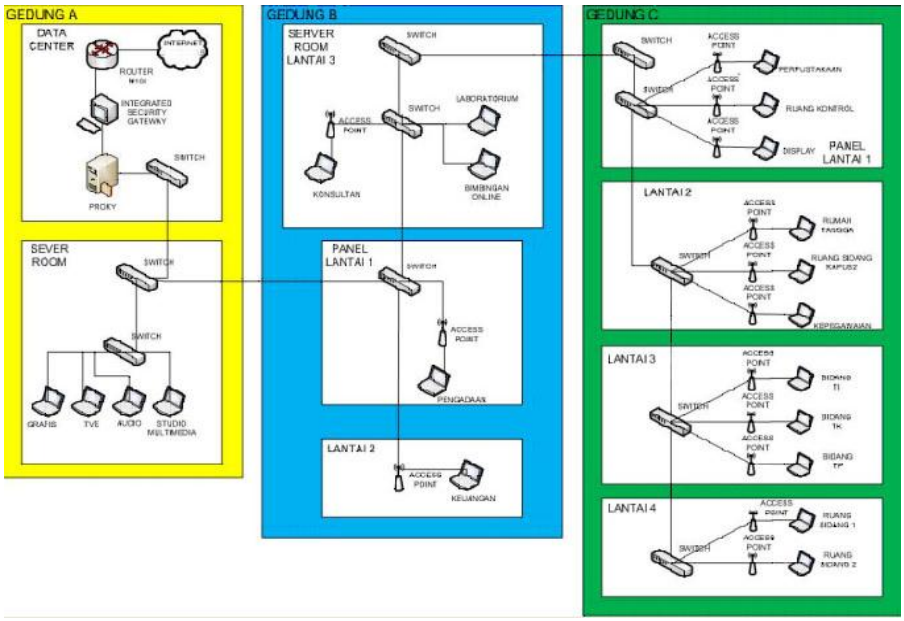
Proyek ini akan banyak membutuhkan banyak peralatan material. Sehingga banyak biaya yang dibutuhkan. Peralatan yang akan di pergunakan akan di terangkan pada bagian yang lain.

3.4.3 Sumber Daya Biaya

Biaya yang di keluarkan dalam proyek ini sudah ditetapkan dan diperhitungkan, Dan juga di dukung oleh kondisi keuangan di DISKOMINFO yang dinilai mampu sanggup untuk megelola kebutuhan biaya dengan baik.

3.5 Jaringan Diskominfo

Diskominfo (Dinas komunikasi dan informatika) adalah instasi pemerintahan yang bergerak di bidang informatika dan komunikasi, dalam infrastrukturnya bangunan diskominfo terbagi dari 3 gedung, sehingga dalam infrastruktur jaringanya lannya dapat di lihat sebagai berikut :



Gambar 3.2 Jaringan lan diskominfo

Gambar di atas merupakan gambaran jaringan secara sederhana. Pada Lantai satu infrastruktur jaringanya terdapat 1 buah ruangan internet publik, yang di dalamnya terdiri dari 10 buah komputer *client*,dan 20 lebih *client* yang tersebar ke beberapa ruangan-ruangan setiap bagian, pada lantai dua terdapat 20 lebih *client* yang tersebar dan di gunakan di setiap ruangan, dan pada lantai tiga terdapat 40 lebih komputer yang tersebar di setiap ruangannya masing-masing. Adapun analisis tentang data *traffic* atau lalu lintas data adalah sebagai berikut :

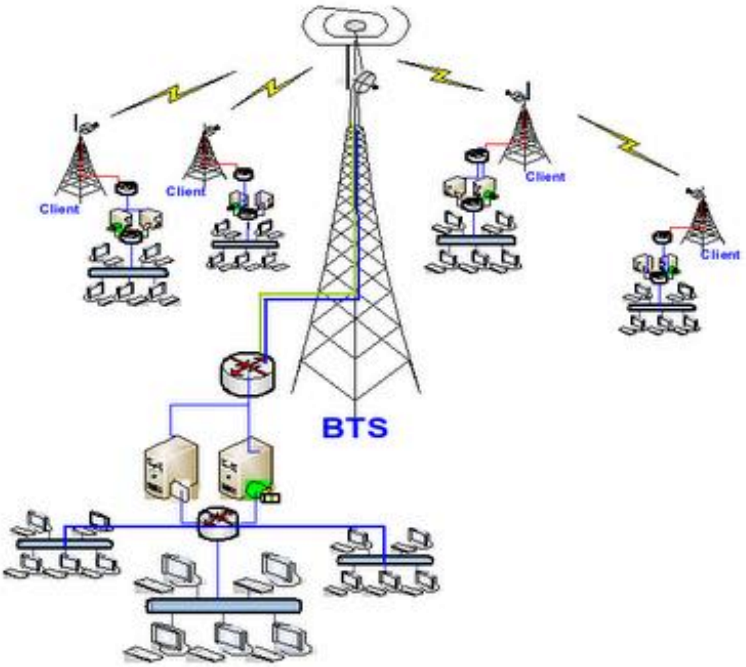
Tabel 3.3 Aktifitas

No	**Jenis Aktifitas**	**Volume per Transaksi (Kbps)**	**Frekuensi Trafik Perhari (Kbps)**	**Volume Trafik Perhari (Kbps)**
1	Cek dan update database di webhosting dari DISKOMINFO dan SOPD setiap ada transaksi informasi ataupun permintaan layanan ataupun Layanan Teknik.	25	1000	25000
2	Cek dan update database di DISKOMINFO dari DISKOMINFO dan SOPD setiap ada transaksi informasi ataupun permintaan layanan ataupun Layanan Teknik.	25	1000	25000
3	Sinkronisasi database di webhosting dan DISKOMINFO	100	17280	1728000
4	Email forwarding dari webhosting ke DISKOMINFO dan SOPD	10	5000	50000
5	Browsing ke webserver dari tiap PC	100	10000	1000000
6	Laporan transaksi informasi perhari melalui email ke DISKOMINFO	2000	2	4000
7	Mengirim email balasan ke masyarakat	25	500	12500
Jumlah				**2844500**

3.6 *Study* kasus

Dalam studi kasus ini akan membandingkan kedua metode pembangunan jaringan yang berbeda sehingga akan terlihat mana yang lebih cocok dalam penerapan pembangunan jaringana yang akan di gunakan.

3.6.1 Jaringan *Wireless*



Gambar 3.3 Jaringan wireles

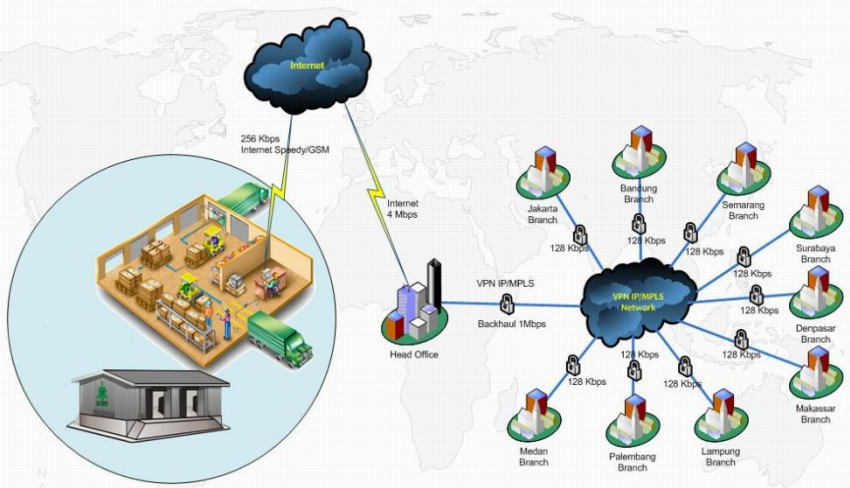
Seperti terlihat di gambar merupakan jaringan wireless dimana jaringan yang terlihat di gambar bisa di katakan jaringan WAN atau GAN, adapaun kelebihan dan kekuranganya menggunakan jaringan ini yaitu :

1. Dalam pengimplementasiannya lebih sulit karena harus mendirikan Tower atau BTS.

2. Biaya yang di butuhkan akan sangat besar, karena di setiap *client* dibutuhkan satu buat tower untuk meletakan akses-point dan radio untuk memancarakan gelombangnya
3. Akses data mudah terganggu, karena model jaringan wireless seperti ini rawan terhadap cuaca, seprti bila sedang hujan, makan sinyal yang akan diterima oleh *client* akan terganggu.
4. Jarak jangkau wireless cukup terbatas.

Maka dalam pembangunan ini tidak terlalu cocok karena yang akan di hubungkan adalah berbagai instansi yang mempunyai jarak cukup jauh dan banyak serta proses penerapannya yang tidak mudah.

3.6.2 Jaringan VPN-IP



Gambar 3.4 Jaringan VPN-IP

Seperti yang terlihat di gambar merupakan jaringan yang menggunakan metode VPN-IP MPLS yang menghubungkan instansi antar kota, jaringan ini menggunakan jaringan yang telah ada seperti jaringan internet, jalur data yang di

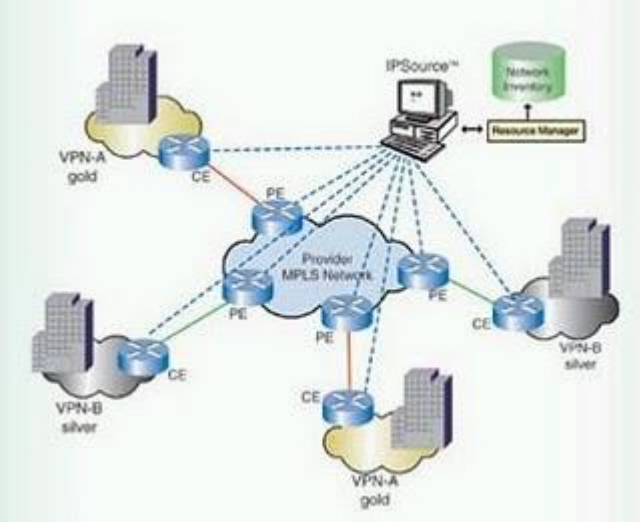
gunakan yaitu *private* bukan untuk public sehingga dimana pun *client* dapat berkomunikasi dengan metode ini. Adapun kelebihan dan kekurangannya yaitu :

1. Mampu mengimplementasikan QoS (*Quality of Service*), yaitu pelanggan dapat menggunakan berbagai jenis aplikasi baik berupa aplikasi yang *Delay Sensitive, Mission Critical* maupun *Non Mission Critical* pada satu *platform* jaringan *privat* IP MPLS.
2. Layanan *multi service*, baik layanan data, video maupun suara. Mendukung berbagai macam aplikasi bisnis : seperti ERP, CRM. Dapat dengan mudah diintegrasikan dengan internet. Memiliki keragaman akses *last mile* (*dial up, dedicated* maupun *wireless*).
3. Skala *Provisioning* yang *fleksibel*. Mudah jika ingin menambah lokasi dan aplikasi baru. Kemudahan membangun jaringan dari kecil ke besar (*gradual migration*). Sederhana dan cepat untuk mengkonfigurasi ulang (tidak membutuhkan '*site to site configuration*'). POP Nasional.
4. Pengendalian yang mudah. *End to end manageable*. NMS tunggal. Mudah digunakan (*user friendly*). Laporan berbasis web (*real time*).
5. Peluang Penghematan Biaya. Tarif tidak berdasarkan jarak. CPE dikelola oleh TelkomMengurangi ketergantungan pada SDM yang ahli (diserahkan pada provider)

Sehingga dengan begitu cukup jelas dengan menggunakan metode jaringan ini akan memudahkan dalam pembangunan serta penghematan biaya dalam proses pembagunan jaringin ini.

3.7 Metode pembangunan jaringan

Metode yang digunakan dalam pembangunan ini yaitu dengan menggunakan VPN IP MPLS, disebutkan sebagai suatu layanan komunikasi data *any to any connections* berbasis *IP Multi Protocol Label Switch* dengan menggunakan peralatan *(hardware)* dari perusahaan *Cisco* (berupa *Cisco Router* dan *Cisco Switch Catalist*). Layanan ini memiliki kelebihan dibandingkan dengan layanan komunikasi data melalui *Leased Line* maupun *Frame Relay* yang menggunakan teknologi yang lebih tua.



Gambar 3.5 jaringan VPN-IP-MPLS

Teknologi VPN IP MPLS merupakan suatu layanan yang dibangun di atas *Integrated Network Architecture* yang secara dinamis dapat mengenali jenis aplikasi *enterprice* untuk memperoleh layanan *end to end security, performance* dan *aviability.* Teknologi VPN IP MPLS ini merupakan solusi yang sangat praktis bagi suatu institusi yang menginginkan komunikasi secara terus menerus (intensif) antara kantor-kantor cabang dengan kantor pusatnya. VPN IP MPLS

digunakan untuk merealisasikan *Class of Service* (CoS), dimana suatu institusi dapat mengimplementasikan aplikasinya baik berupa aplikasi yang memiliki *Delay Time Sensitive*, *Mission Critical* maupun *Non Mission Critical* pada satu *platform* jaringan *private* IP MPLS. Jaringan VPN IP MPLS biasanya di peruntukan untuk :

1. Perusahaan yang memiliki banyak cabang dan menyebar.
2. Perusahaan yang memiliki *configurasion network multi hub/full mesh*.
3. Perusahaan yang menjalankan multi aplikasi.
4. Perusahaan yang memilih *outsourcing* untuk pengaturan *network* nya.

3.8 Sasaran

Sasaran yang ditujukan bagi instansi dinas pemerintahan di lingkungan jawa barat, yang terbagi dari beberapa dinas, Sasaran Awal dari pembuatan jaringan ini adalah :

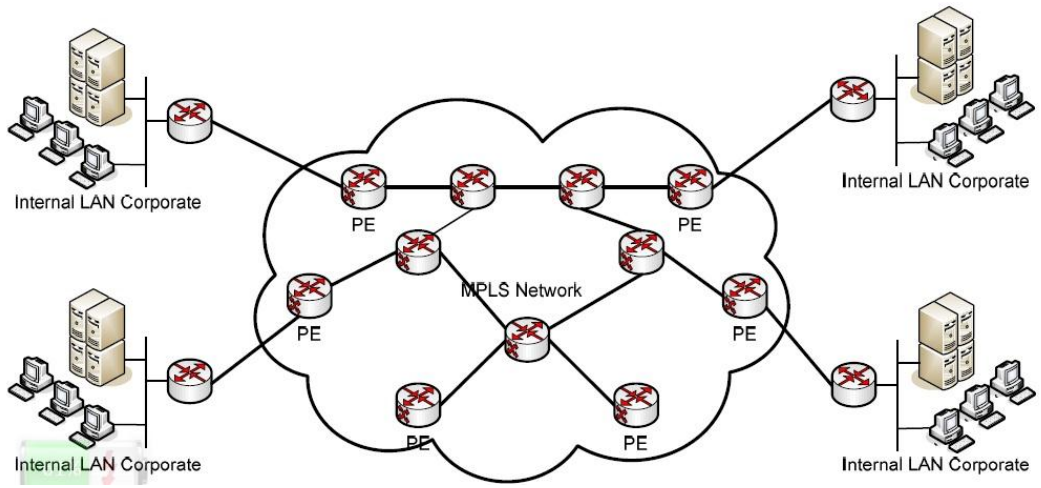
1. Merencanakan konsep dari proyek yang akan dibangun.
2. Merencanakan dengan jelas tujuan dan manfaat dari proyek.
3. Merencanakan pembentukan manager proyek dan tim pelaksanaan proyek.
4. Melakukan peninjauan lokasi pembangunan proyek.

Setelah dilalukan semua sasaran, maka ditentukan temat untuk dijadikan sasaran proyek. Terutama lokasi jaringan yang akan dibangun, yaitu sistem jaringan pada tempat yang akan di kelola kembali dan prasarana daya baik materi, manusia biaya dan waktu Setelah merencanakan dan mendefinisikan

pekerjaan atau aktifitas yang dibutuhkan dalam pembangunan proyek jaringan internet ini.

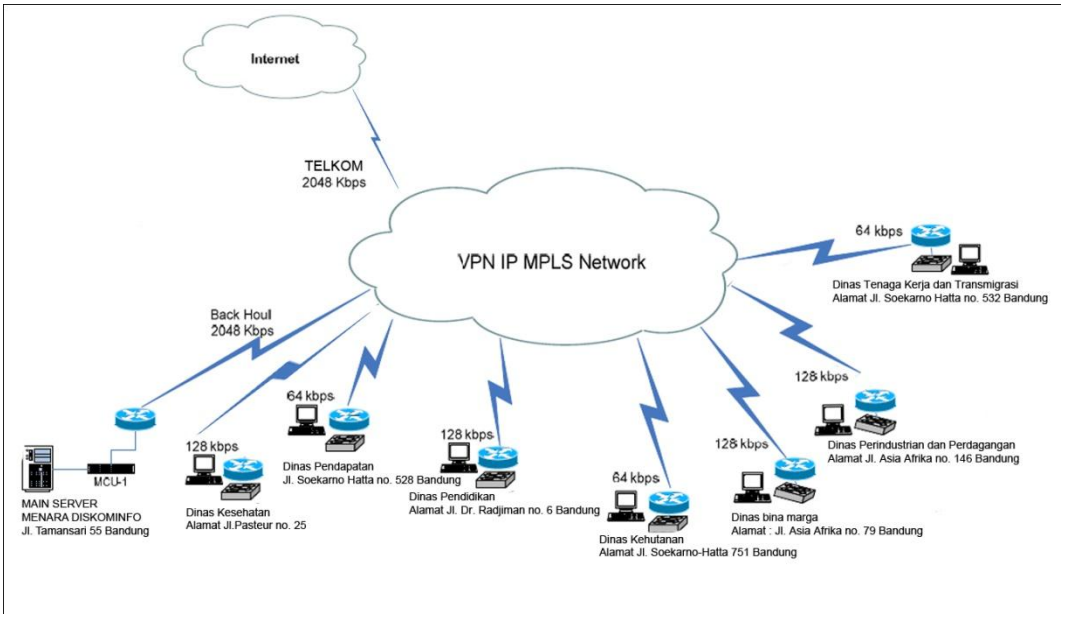
3.9 Implementasi Proyek

Setelah kita menentukan metode yang akan di gunakan dalam pembangunan jaringan sebelumnya, maka pada tahap ini penerapan implementasi yang akan di lakukan. Pada gambar bawah ini penulis akan jelaskan mengenai konfigurasi yang diberikan oleh Telkom untuk produk layanan VPN IP MPLS yang akan di gunakan oleh Diskominfo.



Gambar 3.6 Konfigurasi Infrastuktur *VPN IP MPLS*

Pada gambar di atas Telkom menyediakan sekumpulan *Network* MPLS untuk di gunakan oleh *client*nya, *Network* yang di gunakan menggunakan jalur data yang telah di sediakan oleh Telkom yang tersebar seluruh indonesia, yang kemudian di bagikan kepada *client* yang akan menggunakanya termasuk Diskominfo. Secara umum koneksi jaringan yang akan terbentuk dengan menggunakan teknologi VPN IP MPLS tersebut dapat di lihat pada gambar di bawah berikut.



Gambar 3.7 VPN IP MPLS Network tersebar ke SOPD

dapat kita perhatikan bahwa setiap Dinas terhubung secara langsung menggunakan jaringan *VPN IP MPLS* milik Telkom agar dapat saling terkoneksi dengan Menara Diskominfo yang dalam hal ini difungsikan sebagai sisi *backhole* (pusat interkoneksi jaringan di Diskominfo). Pemanfaatan jaringan VPN tersebut dapat dimanfaat kan untuk kebutuhan-kebutuhan internal Diskominfo seperti pembangunan intranet yang dapat membuat suatu sisten informasi *online* berbasis *web*, komunikasi data maupun suara menggunkan *Instant Messenger (Net Meeting, Office Communicator / Live Communication System*, dll), *sharing resource (file, software dan hardware)*, bahkan sampai dengan pemanfaatan komunikasi menggunakan teknologi *Voice Over Internet Protocol (*VOIP*)*.

Teknologi VPN IP MPLS ini melikiki dua macam *interface* untuk keluaran yang menghubungkan antara *Router PE* yang ada disisi Telkom (Pada

masing-masing STO Telkom yang terdekat dengan Dinas terkait) dengan *Router CE* yang ada di masing-masing Dinas, yaitu :

1. *Standard Ethernet* (10/100 Mbps) yang merupakan keluaran untuk *VPN IP Modem/Router (HDSL Modem).*
2. *Port* V.35 yang merupakan keluaran untuk ke *router* yang akan di terapkan.

Pada perangkat *router* yang terdapat disisi Dinas (CE) terdapat dua macam merk *router* yang digunakan, yaitu : *Cisco Router* dan *Allied Telesyn (AT) Router*. Pada sisi *backhoule*, yaitu menara Diskominfo menggunakan *Cisco Router* 2801 tipe Modular. Pada dinas-dinas yang menggunakan *interface* keluaran berupa *Port* V.35 menggunakan *Cisco Router* 2501 untuk dapat terkoneksi dengan Router yang ada pada sisi *backhole*. Pada Dinas-Dinas yang tersebat menggunakan Router *Allied Telesyn (AT) Router* Tipe AT-AR410 *Multiprotocol Modular Router* 4 X 10/100TX + 1 PIC Slot untuk dapat terkoneksi dengan Router yang ada pada sisi *backhole*. Seluruh Dinas menggunakan *interface* keluaran *Standard Ethernet* menggunakan *VPN IP Modem/Router (HDSL Modem)* dengan Merk ZyXEL Prestige 700 Series untuk dapat terkoneksi dengan Router yang ada pada sisi *backhole*.

3.9.1 Tahapan Implementasi *VPN* Dengan VPN IP MPLS

Adapun tahapan untuk mengimplementasikan VPN dengan VPN IP MPLS adalah sebagai berikut :

1. Membangun infrastuktur jaringan VPN yang menghubungkan semua lokasi Dinas dengan menara Diskominfo sebagai *backhole*.
2. Setelah seluruh infrastruktur jaringan VPN selesai dibangun, langkah berikutnya adalah membangun *Server-Server* yang akan digunakanuntuk melayani kebutuhan yang ada di internal Diskominfo yang ada pada sisi Diskominfo Menara Diskominfo yang akan dijadikan pusat untuk pelayanan, misalnya : *Server* untuk pengaturan sistem domain *(Domain Controller Server), Database Server*, *Domain Name System (*DNS*) Server*, WINS *Server*, DHCP *Server*, Web *Server*, Mail *Server*, Proxy *Server*, dll. Sedangkan untuk pada sisi Dinas keseluruhan, akan di buat minimal ada satu buah *Server* yang dipergunakan sebagai *Additional Domain Controller Server* yang juga difungsikan sebagai Domain Name System (DNS) *Server*, WINS *Server*, dan DHCP *Server*.
3. Setelah infrastruktur dan *server-server* yang akan digunakan siap untuk dipergunakan, maka langkah terakhir adalah untuk membangun aplikasi *online* yang dapat secara *multi user* digunakan dari masing-masing Dinas seperti : Pertukaran data antar dinas, video conference antar dinas, dll.

Pada Diskominfo serta SOPD Kemudian akan di bangun suatu mesin yang disebut dengan *WINS Server*. Mesin *WINS Server* ini juga bangun pada seluruh SOPD. Mesin-mesin *WINS Server* ini nantinya akan selalu melakukan sinkronikasi dengan mesin-mesin *WINS Server* yang lain ketika terjadi sinkroniksai antar mesin *Domain Controller Server*. Tugas dari mesin ini adalah untuk menterjemahkan *Computer Name* atau *NetBIOS Name* menjadi *IP Address* agar dapat diakses dari lokasi lain yang memiki *IP Address* yang berbeda *segment*.

IP Address yang di-*subnetting* disini adalah jaringan komputer yang ada pada suatu instutitusi tersebut menggunakan *IP Address Private*. Kemudian *IP Address Private* tersebut yang tadinya hanya memiliki satu buah *Network ID* dan hanya bisa digunakan satu jaringan komputer yang terdapat pada satu cabang, maka *IP Address Private* tadi dipecah-pecah lagi dengan mengorbankan beberapa *Host ID*-nya untuk membentuk beberapa *Network ID* yang baru. Dengan memiliki beberapa *Network ID* yang baru tadi, maka setiap cabang yang memiliki *IP Address* yang berbeda *segment* (Karena sudah di-*subnetting* tadi), maka sekarang masing-masing IP Address tersebut sudah dapat saling berkomunikasi dengan cabang lain yang memiliki *IP Address* yang berbeda dengan bantuan perangkat *Router*. Sebagai contoh :

Network ID 172.16.0.0/16. Maka *range IP Address* yang dapat gunakan adalah 172.16.0.0 sampai dengan 172.16.255.254 dengan *subnet mask* 255.255.0.0 (/16). Dengan kata lain, dalam satu cabang pada instritusi hanya boleh memiliki maksimal 65.534 *host*. Sementara seperti SOPD, memiliki 10 lokasi yang semua jaringan komputernya terhubung melalui VPN IP MPLS.

Secara teori memang bisa saja anda memberikan *IP Addrress* yang berbeda untuk setiap cabang, misalnya :

IP Address 172.16.0.0/16 untuk Dinas Perkebunan, *IP Address* 172.17.0.0/16 untuk Dinas Kesehatan, *IP Address* 172.18.0.0/16 untuk BSI Pendidikan dan seterusnya. Hal ini dalam konsep intranet kurang tepat. Dalam konsep intranet lebih baik anda menggunakan *Network ID* 172.16.0.0/16 yang *subneting* menjadi beberapa *Netwok ID* baru. Daftar hasil *subnetting IP Address* 172.16.0.0/16 tersebut dapat dilihat pada tabel di bawah ini.

Tabel 3.4 Subnetting IP Address

No	Network ID	Range IP Address	IP Address Broadcast	No	Network ID	Range IP Address	IP Address Broadcast
1	172.16.4.0	172.16.4.1 - 172.16.7.254	172.16.7.255	32	172.16.128.0	172.16.128.1 - 172.16.131.254	172.16.131.255
2	172.16.8.0	172.16.8.1 - 172.16.11.254	172.16.11.255	33	172.16.132.0	172.16.132.1 - 172.16.135.254	172.16.135.255
3	172.16.12.0	172.16.12.1 - 172.16.15.254	172.16.15.255	34	172.16.136.0	172.16.136.1 - 172.16.139.254	172.16.139.255
4	172.16.16.0	172.16.16.1 - 172.16.19.254	172.16.19.255	35	172.16.140.0	172.16.140.1 - 172.16.143.254	172.16.143.255
5	172.16.20.0	172.16.20.1 - 172.16.23.254	172.16.23.255	36	172.16.144.0	172.16.144.1 - 172.16.147.254	172.16.147.255
6	172.16.24.0	172.16.24.1 - 172.16.27.254	172.16.27.255	37	172.16.148.0	172.16.148.1 - 172.16.151.254	172.16.151.255
7	172.16.28.0	172.16.28.1 - 172.16.31.254	172.16.31.255	38	172.16.152.0	172.16.152.1 - 172.16.155.254	172.16.155.255
8	172.16.32.0	172.16.32.1 - 172.16.35.254	172.16.35.255	39	172.16.156.0	172.16.156.1 - 172.16.159.254	172.16.159.255
9	172.16.36.0	172.16.36.1 - 172.16.39.254	172.16.39.255	40	172.16.160.0	172.16.160.1 - 172.16.163.254	172.16.163.255
10	172.16.40.0	172.16.40.1 - 172.16.43.254	172.16.43.255	41	172.16.164.0	172.16.164.1 - 172.16.167.254	172.16.167.255
11	172.16.44.0	172.16.44.1 - 172.16.47.254	172.16.47.255	42	172.16.168.0	172.16.168.1 - 172.16.171.254	172.16.171.255
12	172.16.48.0	172.16.48.1 - 172.16.51.254	172.16.51.255	43	172.16.172.0	172.16.172.1 - 172.16.175.254	172.16.175.255
13	172.16.52.0	172.16.52.1 - 172.16.55.254	172.16.55.255	44	172.16.176.0	172.16.176.1 - 172.16.179.254	172.16.179.255
14	172.16.56.0	172.16.56.1 - 172.16.59.254	172.16.59.255	45	172.16.180.0	172.16.180.1 - 172.16.183.254	172.16.183.255
15	172.16.60.0	172.16.60.1 - 172.16.63.254	172.16.63.255	46	172.16.184.0	172.16.184.1 - 172.16.187.254	172.16.187.255
16	172.16.64.0	172.16.64.1 - 172.16.67.254	172.16.67.255	47	172.16.188.0	172.16.188.1 - 172.16.191.254	172.16.191.255
17	172.16.68.0	172.16.68.1 - 172.16.71.254	172.16.71.255	48	172.16.192.0	172.16.192.1 - 172.16.195.254	172.16.195.255
18	172.16.72.0	172.16.72.1 - 172.16.75.254	172.16.75.255	49	172.16.196.0	172.16.196.1 - 172.16.199.254	172.16.199.255
19	172.16.76.0	172.16.76.1 - 172.16.79.254	172.16.79.255	50	172.16.200.0	172.16.200.1 - 172.16.203.254	172.16.203.255
20	172.16.80.0	172.16.80.1 - 172.16.83.254	172.16.83.255	51	172.16.204.0	172.16.204.1 - 172.16.207.254	172.16.207.255
21	172.16.84.0	172.16.84.1 - 172.16.87.254	172.16.87.255	52	172.16.208.0	172.16.208.1 - 172.16.211.254	172.16.211.255
22	172.16.88.0	172.16.88.1 - 172.16.91.254	172.16.91.255	53	172.16.212.0	172.16.212.1 - 172.16.215.254	172.16.215.255
23	172.16.92.0	172.16.92.1 - 172.16.95.254	172.16.95.255	54	172.16.216.0	172.16.216.1 - 172.16.219.254	172.16.219.255
24	172.16.96.0	172.16.96.1 - 172.16.99.254	172.16.99.255	55	172.16.220.0	172.16.220.1 - 172.16.223.254	172.16.223.255
25	172.16.100.0	172.16.100.1 - 172.16.103.254	172.16.103.255	56	172.16.224.0	172.16.224.1 - 172.16.227.254	172.16.227.255
26	172.16.104.0	172.16.104.1 - 172.16.107.254	172.16.107.255	57	172.16.228.0	172.16.228.1 - 172.16.231.254	172.16.231.255
27	172.16.108.0	172.16.108.1 - 172.16.111.254	172.16.111.255	58	172.16.232.0	172.16.232.1 - 172.16.235.254	172.16.235.255
28	172.16.112.0	172.16.112.1 - 172.16.115.254	172.16.115.255	59	172.16.236.0	172.16.236.1 - 172.16.239.254	172.16.239.255
29	172.16.116.0	172.16.116.1 - 172.16.119.254	172.16.119.255	60	172.16.240.0	172.16.240.1 - 172.16.243.254	172.16.243.255
30	172.16.120.0	172.16.120.1 - 172.16.123.254	172.16.123.255	61	172.16.244.0	172.16.244.1 - 172.16.247.254	172.16.247.255
31	172.16.124.0	172.16.124.1 - 172.16.127.254	172.16.127.255	62	172.16.248.0	172.16.248.1 - 172.16.251.254	172.16.251.255

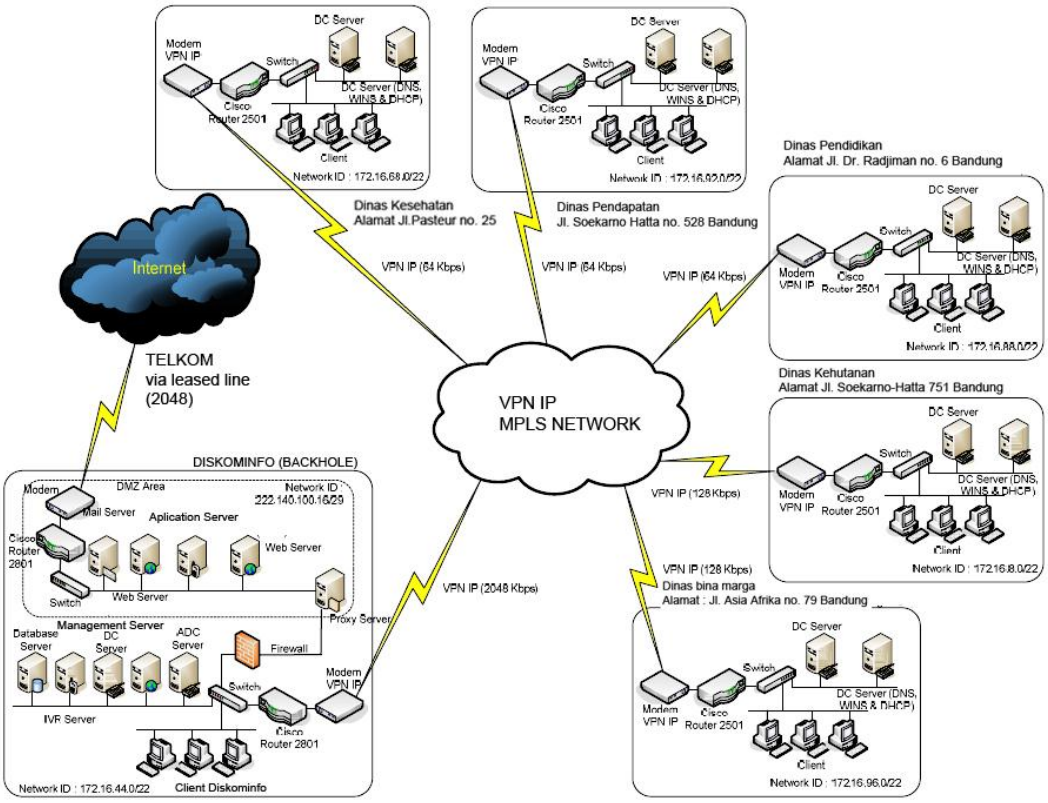
Dari tabel 3.2 dapat disimpulkan bahwa sebuah *Network ID* 172.16.0.0 dengan *default subnet mask*-nya 255.255.0.0 (/16) setelah dilakukan *subnetting* sebanyak 6-*bit* menghasikan 62 *Network ID* baru dan pada setiap *Network ID* maksimal ada sebanyak 1.022 *host*. Kalau anda memiliki sebanyak 62 Network ID, berarti anda dapat menghubungkan maksimal 62 kantor anda ke dalam jaringan komputer *(WAN)*. Adapun ke-62 Netwok ID baru tersebut adalah 172.16.4.0, 172.16.8.0, 172.16.12.0, ..., 172.16.248.0 dengan *subnet mask* yang baru yaitu 255.255.252.0(/22).

Dalam menentukan *IP Address* yang akan digunakan oleh Diskominfo yang akan menghubungkan semua jaringan komputer yang terdapat pada kantor cabang SOPD *(WAN)*, akan menggunakan *IP Address Private*. Hal ini dimaksudkan, apabila suatu saat, SOPD akan melakukan koneksi ke dunia luar *(internet)* maka tidak perlu repot-repot untuk merubah konfigurasi *IP Address* lagi (karena kemungkinan besar *IP Address* yang digunakan sudah ada yang menggunakannya di *internet*). Pada tabel berikut ini adalah rincian daftar *IP Address Private* yang pergunakan di setiap kelasnya.

Tabel 3.5 *IP Address Private*

No	Kelas	Network ID Private	Subnet Mask	Range IP Address
1	A	10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
2	B	172.16.0.0	252.240.0.0	172.16.0.1 - 172.16.255.254
3	C	192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

Adapun Implementasi lengkap jaringan WAN menggunakan VPN IP MPLS antar diskominfo dengan SOPD adalah sebagai berikut :



Gambar 3.8 Implementasi Lengkap via MPLS NETWORK

Pada gambar tersebut dapat anda lihat bahwa setiap SOPD dapat terhubung ke DISKOMINFO menggunakan media VPN IP MPLS, dimana seluruh komputer yang ada dapat terhubung secara langsung antara satu dengan lainnya seolah-olah berada dalam satu jaringan LAN. Prinsip kerja dari VPN IP MPLS tersebut adalah menghubungkan masing-masing SOPD yang ada dengan DISKOMINFO . *Router-router* disini berfungsi untuk melewatkan paket-paket data yang datangnya dari *IP Address* yang berbeda segmen.

Sedangkan agar masing-masing SOPD dapat terkoneksi ke jaringan global *(*internet*),* maka pada konfigurasi *Cisco Router* 2801 yang terdapat pada menara Diskominfo *(Backhole)* harus diberikan pengaturan agar setiap komputer yang akan akses ke internet harus menuju ke *Proxy Server (Squid)* yang ada di *Backhole* dengan *IP Address* 172.16.44.254. Jadi komputer yang boleh langsung terhubung ke *internet* adalah komputer *Proxy Server* yang memiliki dua *Ethernet Card,* yaitu : 172.16.44.254/22 dan 222.140.100.22/29 yang mana *IP Address* 222.140.100.22/29 berada pada area *Demilitary Zone (DMZ)* yang dilindungi oleh *Firewall*.

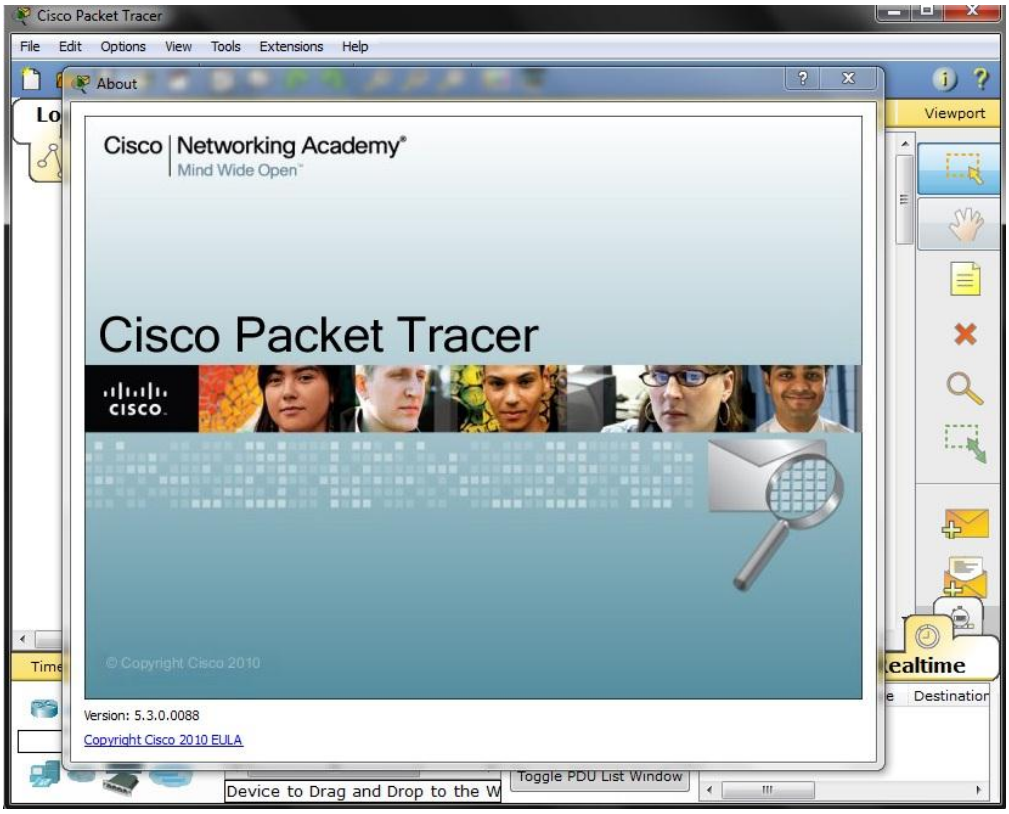
Demilitary Zone (DMZ) meskipin kedengarannya sangat asing, sebenarnya ini hanya area yang berada diambang luar dari *firewall*. Asumsinya bahwa *DNZ* ini adalah halaman depan rumah anda, halaman ini masih milik anda. Anda juga bisa meletakan barang-barang tertentu disana, sementara juga meliki barang-barang yang harus dijaga didalam rumah.

Menurut Rafiudin [2006, Hal. 10], dalam kontek *firewall, DMZ* dapat didefinisikan ”Sebagai bagian dari jaringan namun bukan bagian dari jaringan internal kita dan tidak secara langsung menjadi bagian dari internet. Secara tipikal, area ini berada diantara router akses internet kita dan *Host Bastian* (”Benteng”) kita meskipun dapat juga berada diantara dua komponen pembentuk *pollicy* arsitektur kita.

3.10 Uji Coba

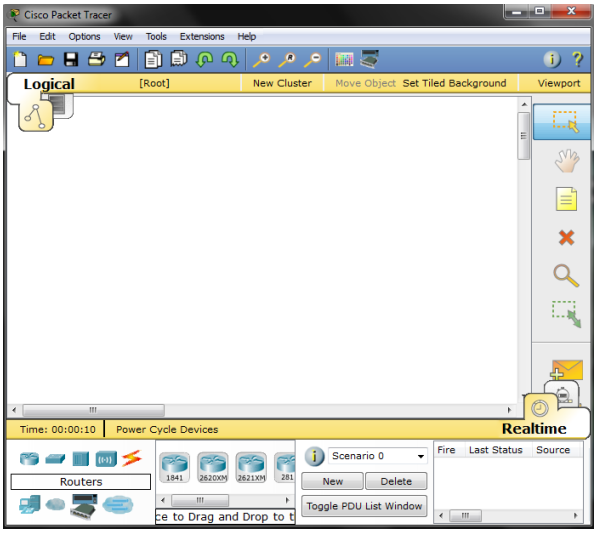
Pada bagian ini merupakan bagian uji coba dari jaringan yang telah di bangun, apakah jalan atau tidak akan terlihat dari command prompt yang menunjukan indikator sukses, untuk uji coba ini akan menggunakan bantuan dari software *CISCO* yang bernama *Packet Tracer* sebagai *software* simulasi untuk pembangunan jaringan, dalam simulasi uji coba ini *ip-address* yang akan di gunakan berbeda pada saat implementasi, sehingga bisa beragam dalam pengalamatan *ip-address* serta kelas yang di digunakan dalam uji coba kali ini, adapun tahap-tahapnya yaitu :

1. Tampilan Cisco Packet Tracer



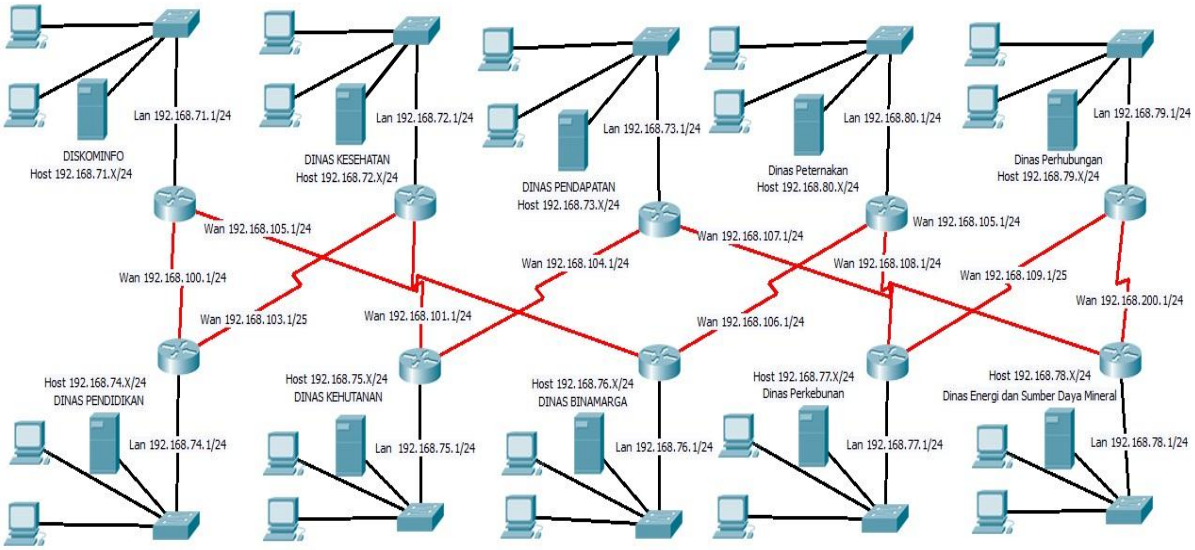
Gambar 3.9 tampilan awal

2. Pilih *New File* untuk memulai



Gambar 3.10 tampilan menu

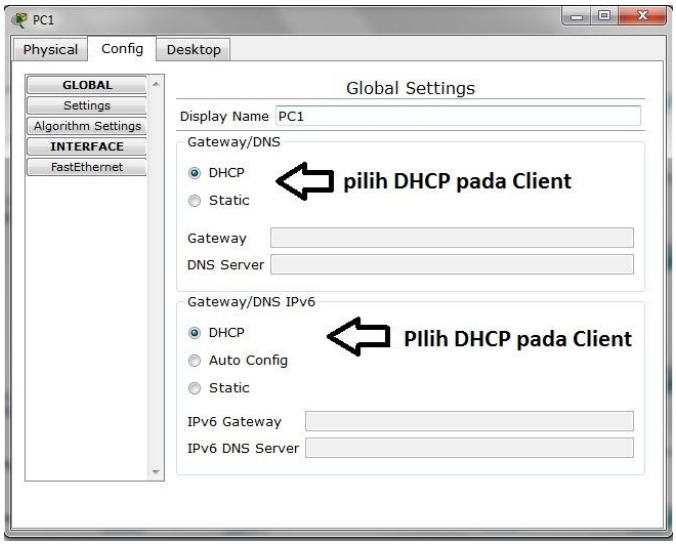
3. Kemudian *design* jaringan yang akan di bangun adalah sebagai berikut :



Gambar 3.11 Design Jaringan

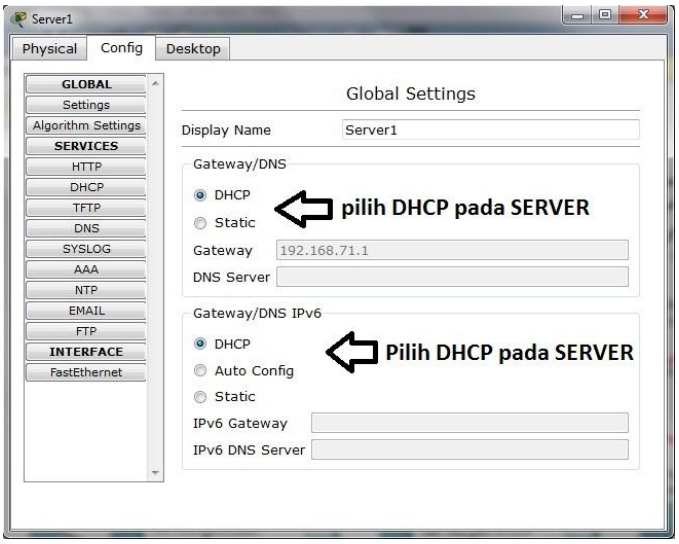
Seperti gambar diatas terdapat 10 SOPD yang tergabung dalam satu ruang lingkup jaringan, di setiap Dinas terdapat satu buat *server* serta *router* untuk menghubungkan segmen *ip-address* yang berbeda kelas.

4. Pada sisi *Client* Diskominfo pilih menu *config* kemudian pilih DHCP, menggunakan DHCP agar lebih memudahkan dalam pendistribusian *ip-address*, mengingat jumlah komputer di setiap instansi tidak sedikit.



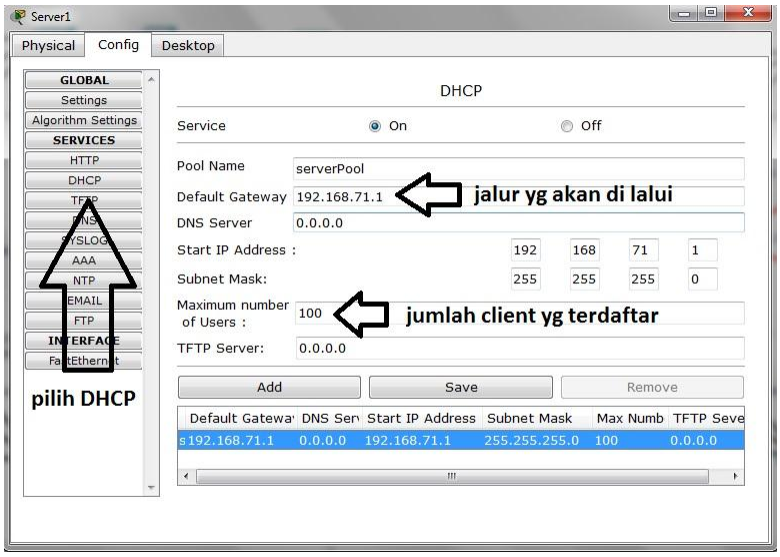
Gambar 3.12 Tampilan Pada *Client*

5. Pada sisi *Server* Diskominfo pilih menu *Config* kemudian pilihlah menu DHCP, untuk membuat pengaturan DHCP kepada *Client*.



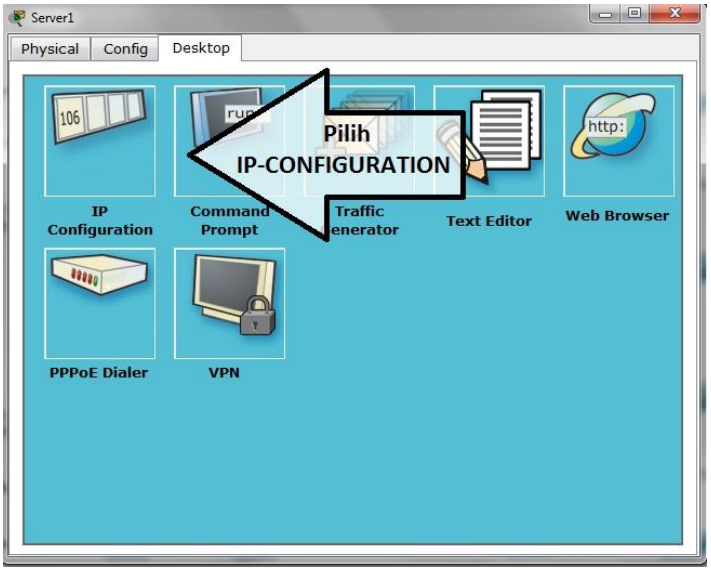
Gambar 3.13 Tampilan pada *Server*

6. Kemudian pilih menu DHCP pada bagian CONFIG dan isikan Default *Gateway* serta *Maximum Number* untuk *Client*



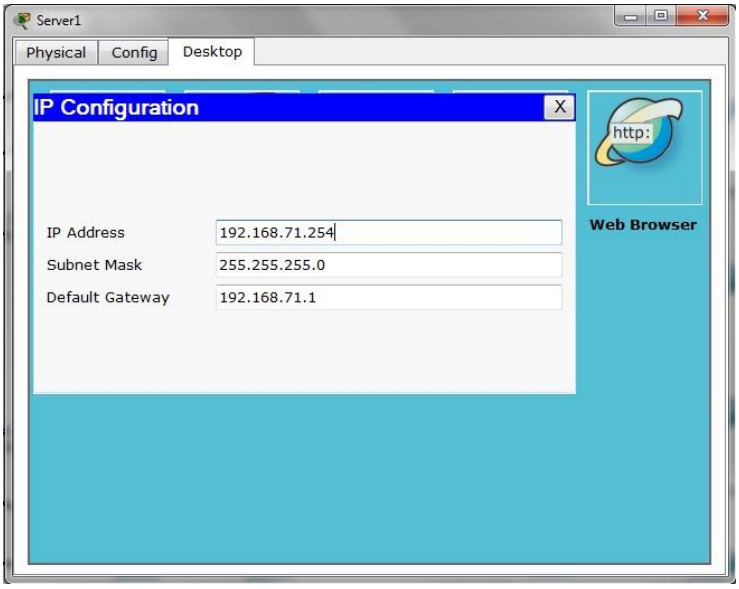
Gambar 3.14 Setting DHCP

7. Kemudian pada bagian *Desktop* pilih *Ip-Configuration* untuk mengatur ip untuk *server*.



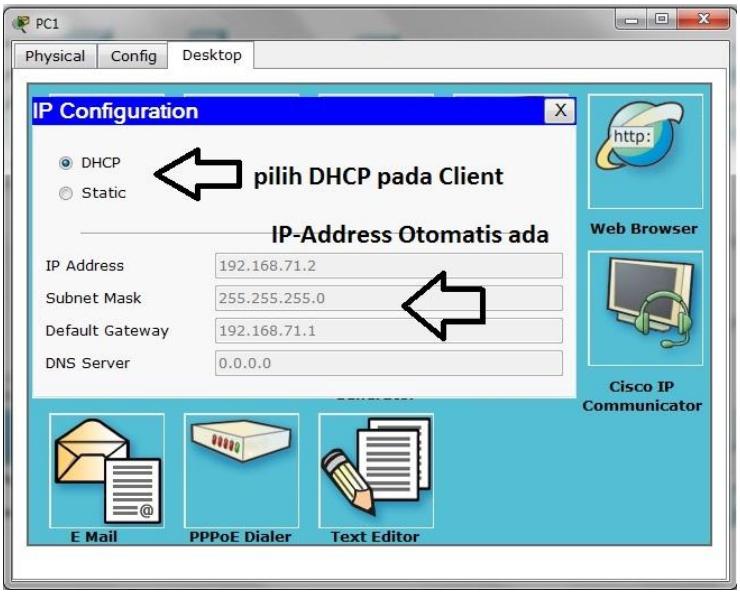
Gambar 3.15 Menu *Ip-Configuration*

8. Kemudan masukan *ip-address* untuk *server* dengan *ip-address*. Untuk *Subnet-id* di setiap *server* pasti akan berbeda dengan *network-id* yang sama.



Gambar 3.16 Memasukan *Ip-Address*

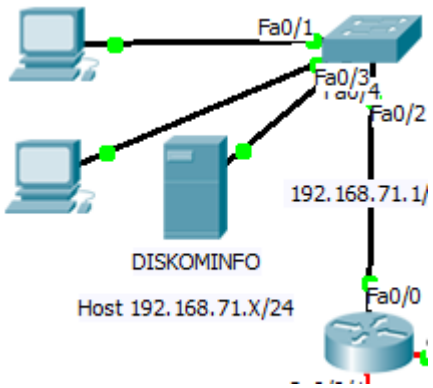
9. Setelah selesai, maka pada sisi *client ip-address* akan terisi secara otomatis, dikarenakan menggunakan dhcp.



Gambar 3.17 Otomatis *Ip-Address* pada *Client*

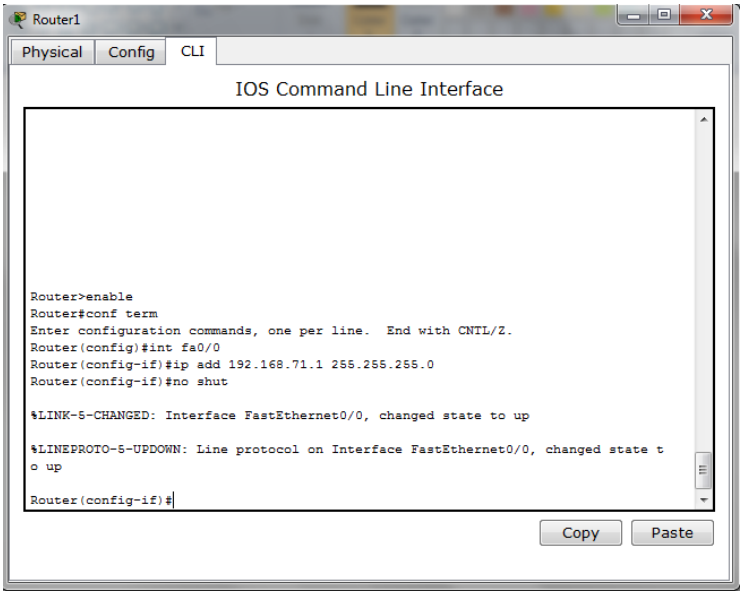
Dari tahap 1-9 Settingan sama di setiap Dinas, untuk settingan dhcp.

10. Kemudian setting pada *router* Diskominfo, Terlihat ada titik warna hijau menandakan *ip-address* teleh terdaftar pada *router* yang di jadikan *gateway* untuk *ip-address* 192.168.71.1, ada pun proses untuk bisa menjadi hijau tersebut bisa di lihat pada tahap ke sebelas.



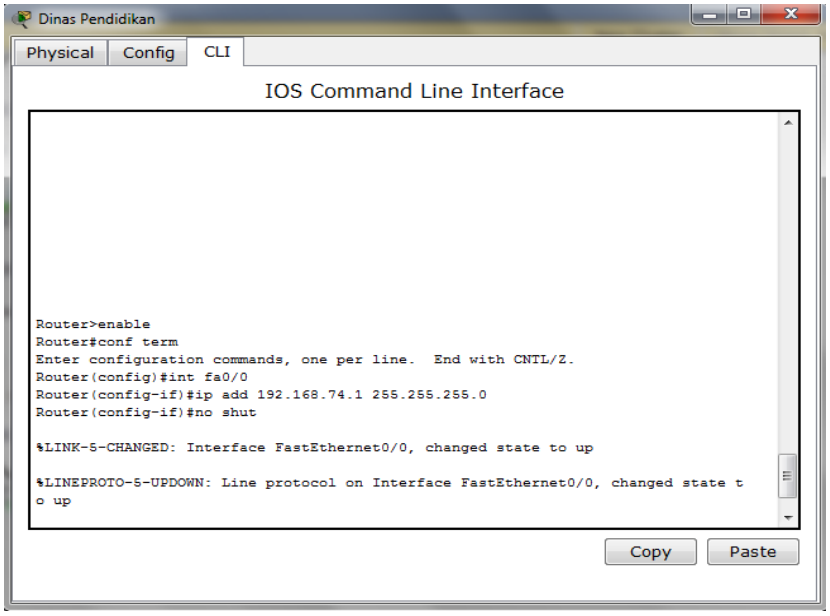
Gambar 3.18 Jaringan Lan dan *Router*

11. terlihat pada gambar merupakan barisan perintah untuk mengaktifkan dan mendaftarkan *ip-address* yang akan di jadikan *gateway* bagi *client* dan *server* yang akan di lalui, bila berhasil makan akan ada tulisan *state to up*.



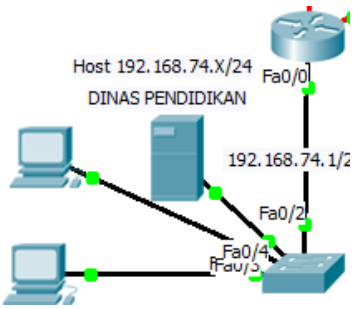
Gambar 3.19 *Command Line Interface Router*

12. Setelah kita melakukan tahap 1-9 yang sama pada sopd yang lain, Kemudian pada setiap *Router* salah satunya Dinas Pendidikan harus di isikan baris perintah seperti gambar, untuk bisa menyambungkan antara *server* dan *client* kepada *router*.



Gambar 3.20 *Command Line Inter*face Dinas Pendidikan

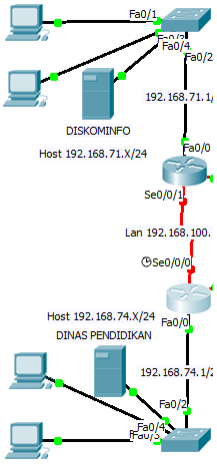
13. Setelah *state to up* maka akan tersambung seperti gambar di bawah ini :



Gambar 3.21 Jaringan Terhubung

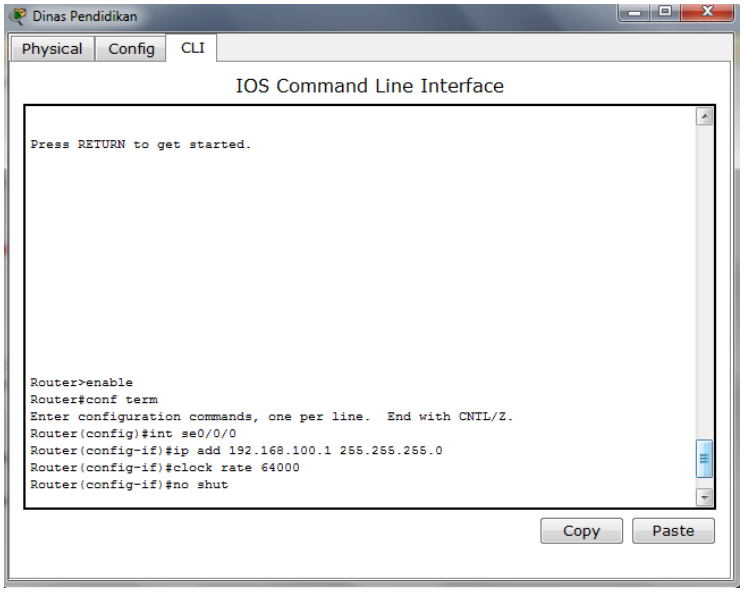
Dari tahap 10-13 settingan sama bagi setiap Dinas untuk menghubungkan Lan dengan *Router*, yang selanjutnya akan di teruskan ke jaringan wan.

14. Kemudian untuk mengkoneksikan dua *network-id* yang berbeda pada setiap Dinas, maka harus di *setting* terlebih dahulu di kedua buah *Router* di Dinas masing masing. Karena pada *line router* masih berwarna merah.



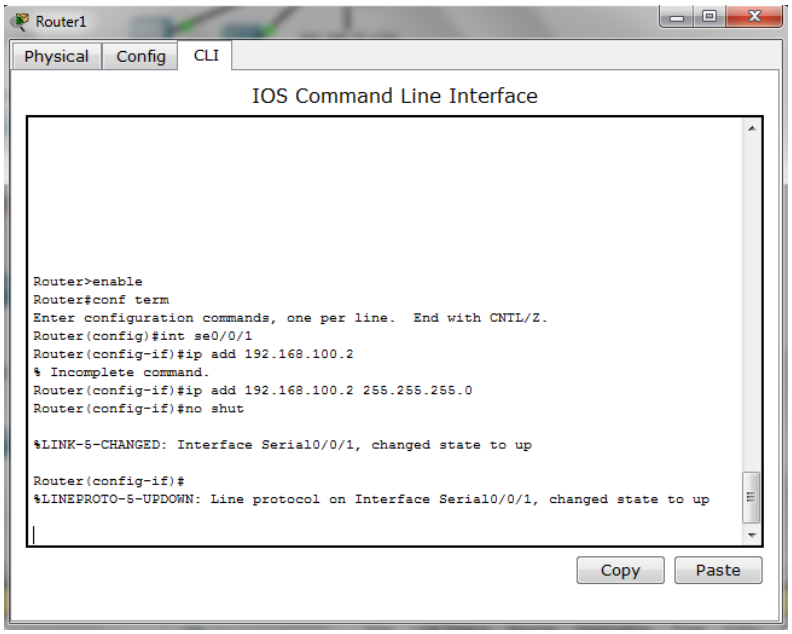
Gambar 3.22 Menghubungkan *Router* yang berbeda

15. Untuk menyambungkanya harus di masukan perintah, disini *router* harus di berikan *ip-address* terlebih dahulu sebagai identitas untuk di daftarkan di *router* dinas yang lain.



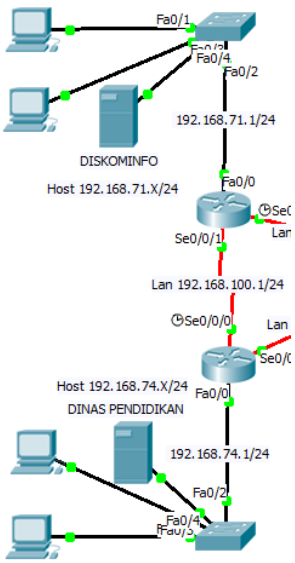
Gambar 3.23 *Command Line Interface* Dinas Pendidikan

16. Dan pada *Router* Diskominfo pun harus di *setting* dengan memasukan perintah seperti berikut :



Gambar 3.24 *Command Line Interface* Dinas Diskominfo

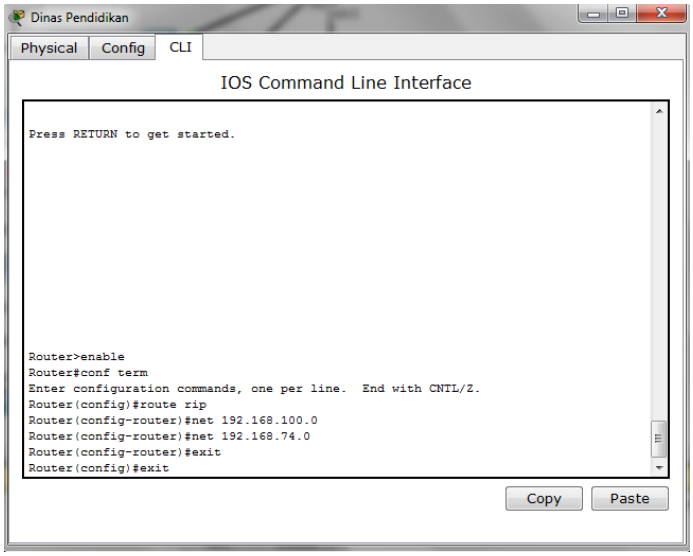
17. Maka hasilnya akan *state to up* dan kedua *router* akan terhubung yang menunjukan tanda warna biru di setiap *line router*.



Gambar 3.25 Jaringan Terhubung

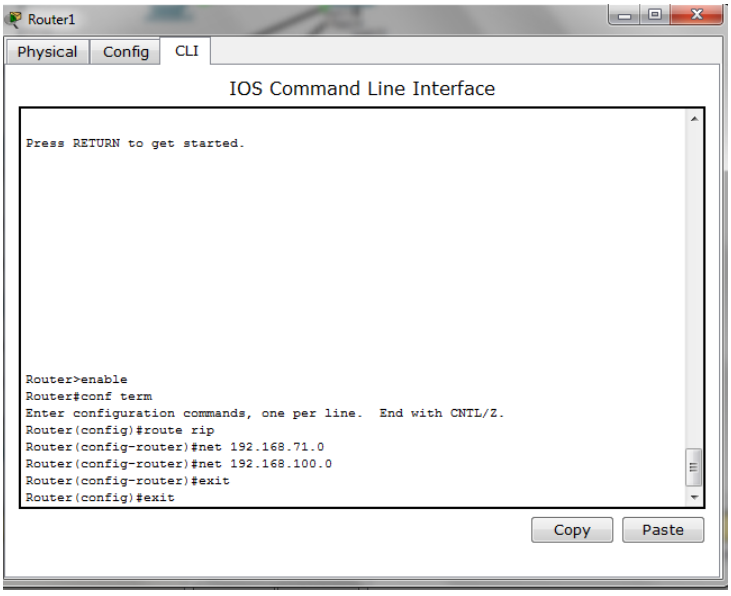
Dari tahap 14-17 Settingan sama untuk menghubungkan *router* yang berbeda.

18. Setelah di setting antar Dinas belum bisa terhubung di karenakan harus di *setting route rip* nya terlebih dahulu yaitu proses pendaftaran *ip-address* pada *line* untuk *client* dan *line* untuk *router* keluar, seperti terlihat di gambar.



Gambar 3.26 *Router Rip* Dinas Pendidikan

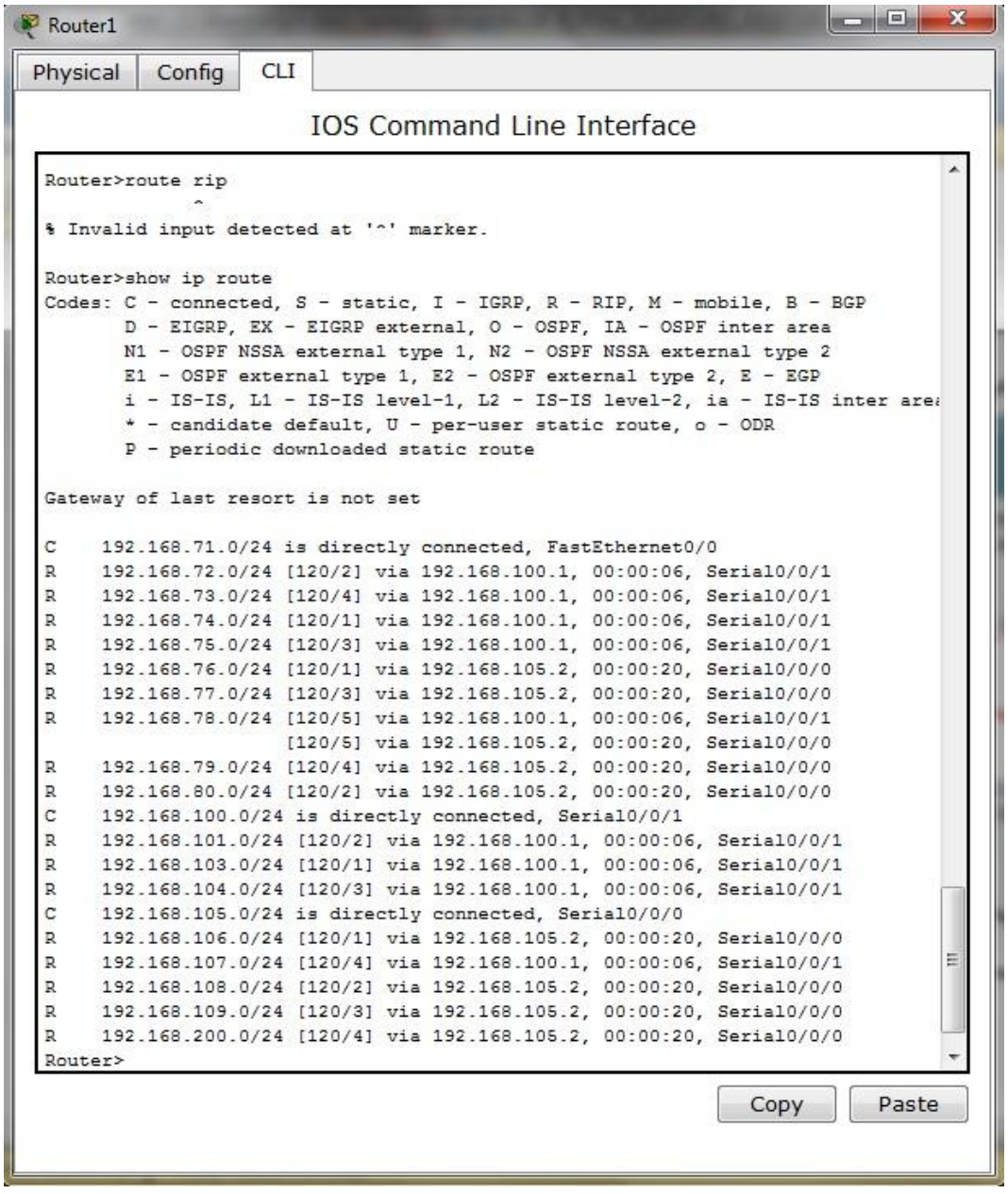
19. Dan begitu juga pada sisi *Router* di Diskominfo *ip-address line* yang masuk dan keluar harus di daftarkan.



Gambar 3.27 *Route Rip* Diskominfo

Dari tahap 18-19 Settingan sama untuk *Router* di setiap Dinasnya.

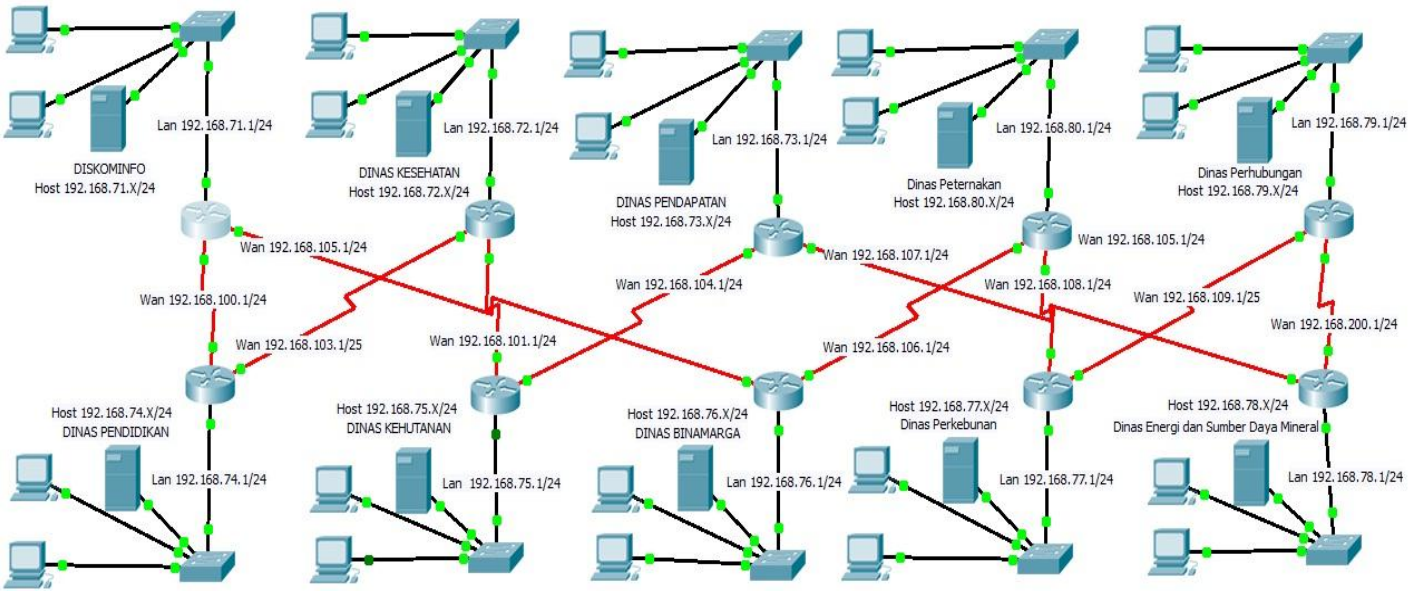
20. Dan proses begitu seterusnya pada sopd yang lain, sehingga dihasilkan *Routing* seperti berikut :



Gambar 3.28 *Routing*

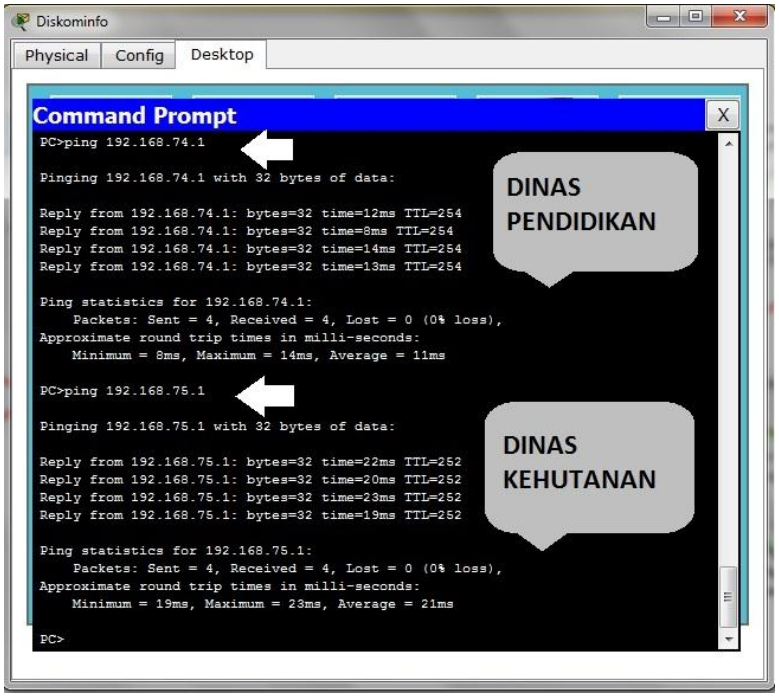
Dari hasil *Routing* tersebut makan dapat di lihat jalur yang di gunakan di setiap *Router*, yang di gunakan pada setiap dinas, sehingga dapat saling terhubung dan berkomunikasi satu dengan yang lainnya.

21. Dan jaringan secara keseluruhan setelah jadi seperti berikut, terdapat *node-node* biru disetiap perangkatnya yang menunjukan telah terhubung.



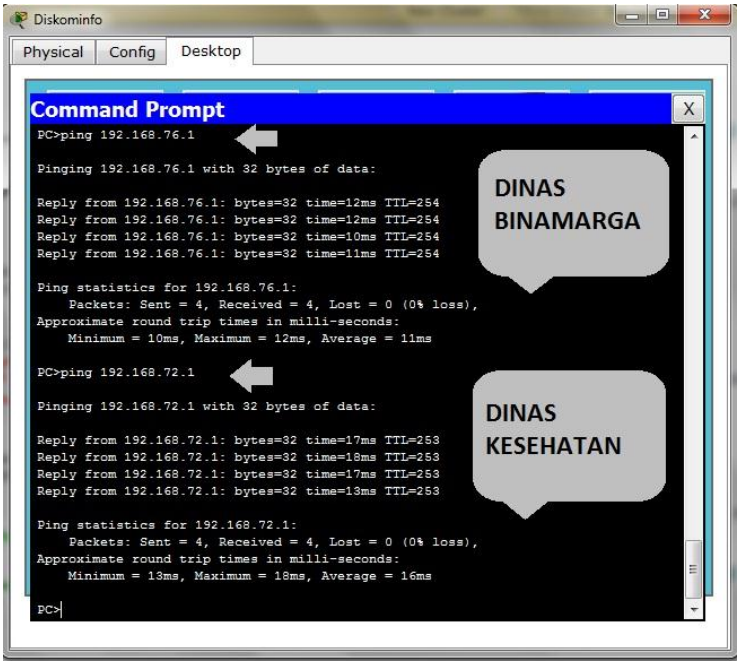
Gambar 3.29 Jaringan keseluruhan terhubung

22. Untuk pengecekan apakah jalan atau tidak maka akan dilakukan *ping* dari Diskominfo ke setiap Dinas yang lain dan hasilnya yaitu :



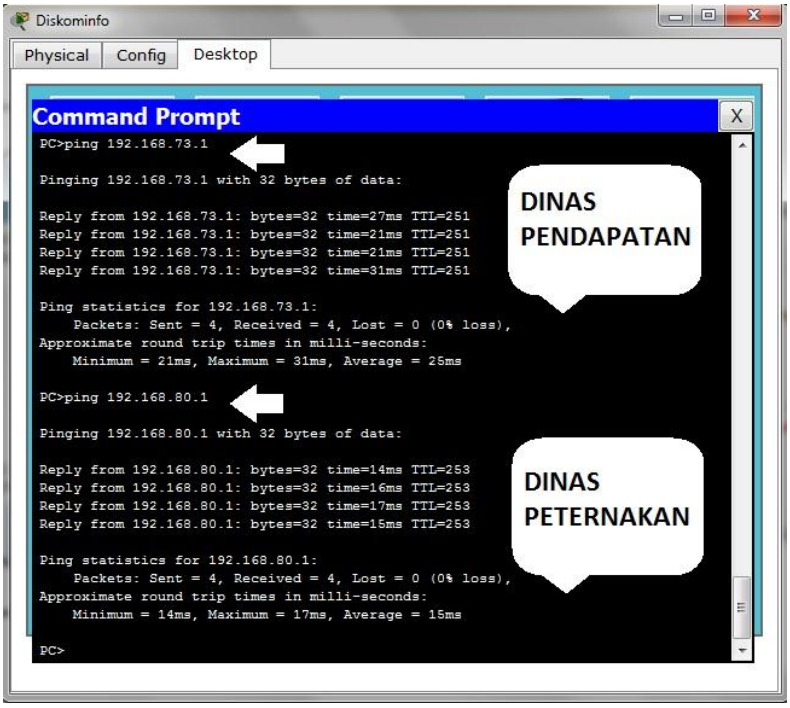
Gambar 3.30 Ping Dinas Pendidikan dan kehutanan

23. Ping dari Diskominfo ke Dinas Binamarga dan Dinas Kesehatan



Gambar 3.31 *Ping* Dinas Binamarga Dan Kesehatan

24. Ping dari Diskominfo ke Dinas Pendapatan dan Dinas Peternakan



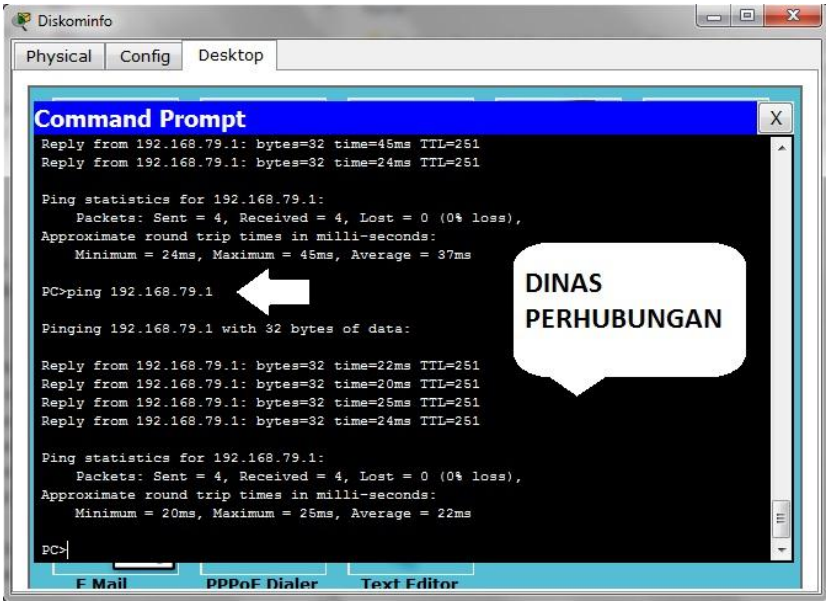
Gambar 3.32 *Ping* Dinas Pendaptan dan Peternakan

25. *Ping* dari Diskominfo ke Dinas Perkebunan dan Dinas Energi dan sdm



Gambar 3.33 *Ping* Dinas Perkebunan Dan sdm

26. *Ping* dari Diskominfo ke Dinas Perhubungan



Gambar 3.34 *Ping* Dinas Perhubungan

Dengan begitu maka semua jaringan telah terhubung sesuai dengan judul laporan yaitu menghubungkan Diskominfo dengan 10 SOPD di lingkungan Provinsi Jawa Barat, seperti yang terlihat di setiap gambar yang ada menunjukan indikator *Reply* yang berarti terkoneksi dan terhubung kepdaa tujuan yang di maksud.

3.11 Jadwal projek

Proyek ini akan memakan waktu 3 bulan, dengan jadwal sebagai berikut :

Tabel 3.6 Jadwal

No	Deskripsi Kegiatan	Bulan ke-1				Bulan ke-2				Bulan ke-3			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Pendefinisian Masalah	√	√										
2	Perancangan Instrumen Proyek	√	√	√									
3	Pembuatan Proyek			√	√	√	√	√	√				
4	Evaluasi Proyek					√	√	√	√				
5	Pengolahan Data						√	√	√	√			
6	Ringkasan Eksekutif									√			
7	Seminar Hasil Proyek										√		
8	Penulisan Laporan Proyek											√	√
9	Implementasi Laporan Proyek												√

3.12 Anggaran Proyek

Pada bagian ini anggaran proyek telah di sediakan oleh Diskominfo (Dinas Komunikasi Dan Informatika) senilai 500 juta, adapun biaya tersebut bisa kami tekan sekecil mungkin sehingga dapat menghemat biaya pembangunan jaringan yang akan di buat tanpa mengurangi kualitas dan hasil yang akan di capai. Adapun rincian biaya, sebagai berikut :

3.13 Biaya Pembelian Peralatan

Tabel 3.7 Biaya Peralatan

NO	NAMA BAHAN	JUMLAH	HARGA SATUAN	JUMLAH
1	Konektor RJ-45	100 Dus	Rp.45000,-/Dus	Rp.4.500.000,-
2	Belden UTP 1000	10 Roll	Rp.300.000,- /roll	Rp.3.000.000,-
3	Pipa Kabel	100 Buah	Rp.30.000,-/Set	Rp.300.000,-
4	Server	11 Buah	Rp.10.000.000,-	Rp.110.000.000,-
5	Broadband Router	11 Buah	Rp. 5.000.000,-	Rp.55.000.000,-
6	Switch Manageable	15 Buah	Rp. 1.500.000,-	Rp.22 500 000,-
9	Mikrotik	11	Rp.3.000.000,-	Rp.33.000.000,-
JUMLAH			**Rp. 228 300 000**	

2. Biaya Pemasangan VPN

Tabel 3.8 Biaya Pemasangan

Class of Service	Description	Application	SLA Parameter	CPE Services
VPN IP Gold	Services to support mission critical which are real time and time dependent: - Intranet - Extranet - Disaster Recovery - Carrier Interconnect	SAP,Siebel, Oracle,Baan, people Soft,Citrix	Network Availability = 99% Latency = 125-150 ms Packet Loss <= 5 %	Managed

VPN IP MPLS Interactive	**Rp. 4.500.000,-**

3. Biaya Pembelian Perangkat Lunak

Tabel 3.9 Biaya Perangkat lunak

NO	SOFTWARE	JUMLAH SATUAN	JUMLAH
1	Microsoft Windows 2008 R2 Server	1 Buah / 15 licence	Rp.20.000.000,-
2	Microsoft Exchange Server	1 Buah / 15 licence	Rp.15.000 000,-
3	Aplikasi dan program-program yang lain	5 Buah	Rp.5.000.000,-
JUMLAH		**Rp.40.000.000,-**	

4. Biaya Pemeliharaan Per Tahun

Tabel 3.10 Biaya Pemeliharaan

NO	SDM AHLI	JUMLAH ORANG	JUMLAH
1	Networking Checking	2 Orang	Rp.6.000.000,-
2	Maintenance Networking	3 Orang	Rp.12.000 000,-
JUMLAH		**Rp.18.000.000,-**	

5. Sehingga jumlah keseluruhan yang di butuhkan adalah

Tabel 3.11 Biaya Keseluruhan

JUMLAH Peralatan	**Rp. 228 300 000**
JUMLAH VPN IP MPLS	**Rp. 4.500.000,-**
JUMLAH Perangkat Lunak	**Rp.40.000.000,-**
JUMLAH Tenaga Ahli	**Rp.18.000.000,-**
JUMLAH	**Rp.290.800.000.00**

6. Anggaran yang di sediakan adalah

Tabel 3.12 Biaya Tersedia

JUMLAH	**Rp.500.000.000.00**

6. Jumlah biaya yang dapat di tekan adalah

Tabel 3.13 Sisa Biaya

JUMLAH	**Rp.209.200.000.00**