BAB III

PEMBAHASAN

3.1 Jadwal Kegiatan Praktek

Kegiatan yang dilakukan selama kerja praktek di PT.PLN (Persero) UPJ Ujung Berung Distribusi Jawa Barat dan Banten yang beralamat di Jalan AH Nasution No. 65 Bandung – 40611 Telp : (022) – 7801502, 7806653. kegiatan kerja praktek dilaksanakan sejak tanggal 1 Agustus 2009 dan berakhir pada tanggal 1 September 2009. Kegiatan kerja praktek dilakukan pada hari senin sampai dengan hari jumat, yang dimulai pada pukul 08.00 WIB dan berakhir pada pukul 14.00 WIB. penulis di tempat kan di divisi/ bagian Cater dan rekening bagian lahta (pengolahan data).

Tabel III. 1 Jadwal kegiatan kerja preaktek

No	Kegiatan	Waktu			
		Minggu ke 1	Minggu ke 2	Minggu ke 3	Minggu ke 4
1	Perkenalan lingkungan kerja				
2	Pengumpulan data-data tentang ruang lingkup pekerjaan				
3	Pengumpulan data-data jaringan komputer di Pln UPJ Ujung Berung				
4	Pengumpulan artikel dan referensi penunjang				
5	Analisis jaringan (LAN dan MAN) di Pln UPJ Ujung Berung				

3.2 Data Kerja Praktek

3.2.1 Komputerisasi di PT.PLN UPJ Ujung Berung

Penggunaan komputer di PT.PLN UPJ Ujung Berung telah menjadi kebutuhan primer, hampir semua divisi menggunakan komputer sebagai alat bantu untuk menyelesaikan pekerjaannaya. Merujuk pada data yang penulis dapat total terdapat 55 unit komputer ditambah 6 unit *server*.semuanya terhubung dalam jaringan lokal (LAN). Selain LAN, PT. PLN (Persero) UPJ Ujung Berung Distribusi Jawa Barat dan Banten juga terhubung dengan *Metropolitan Area Network* (MAN) yang menghubung kan antar UPJ-UPJ yang berada dalam satu kawasan APJ Bandung, tercatat 10 gedung atau kantor yang terhubung dalam wan ini; diantaranya APJ Bandung, Kantor Distribusi, UPJ Ujungberung, UPJ Bandung selatan, UPJ Bandung timur,UPJ Bandung barat,UPJ Bandung utara,UPJ Kopo,UPJ Cijawura dan UPJ Priangan.

3.2.2 Jaringan LAN di PT.PLN UPJ Ujung Berung

3.2.2.1 *Server* dan *Host* yang di miliki

Adapun server yang terdapat di PT.PLN UPJ Ujung Berung

1. *Database server* : di gunakan untuk menyimpan *database.* dengan spesifikasi *Memory* DDR 256 Mb, *Processor* P4 2,26 Ghz , HHD 40 Gb dan mengunkan sistem operasi *Windows 2000 server*.
2. Database aplikasi server : di gunakan untuk menyimpan aplikasi yang di perlukan oleh hampir semua divisi contohnya *CM@X* dan *Backup CM@X*. dengan spesifikasi : *Memory* DDR 1 Gb, *Processor* P4 2.4 Ghz, HHD 160,

Sistem operasi *Windows 2000 server.*

3. *Server* GIS / *Geogratical information System.*

4. *Server* PDT / *Portable Data Terminal* dengan spesifikasi *Memory* DDR 256 Mb, *Processor* P4 2,3 Ghz , HHD 40 Gb dan menggunakan sistem operasi *Windows 2000 server.*

5. Server keuangan : digunakan untuk menyimpan data keuangan dan *up date* PPOB (*Payment Point*) dengan spesifikasi *Memory* DDRII 1 Gb, *Processor dual core*,HHD 80 Gb, menggunakan sistem operasi *Windows* 2000 server

6. Server antivirus : di gunakan untuk menyimpan aplikasi dan *update* antivirus, antivirus yang digunakan yaitu smantek dan Smadav .adapun spesifikasi *Memory* DDRII 1 Gb, *Processor core 2 duo*, menggunakan sistem operasi *Windows 2000 server*

7. *Proxy server* digunakan sebagai modem yang menghubungkan dengan internet dan ke jaringan man seperti APJ.

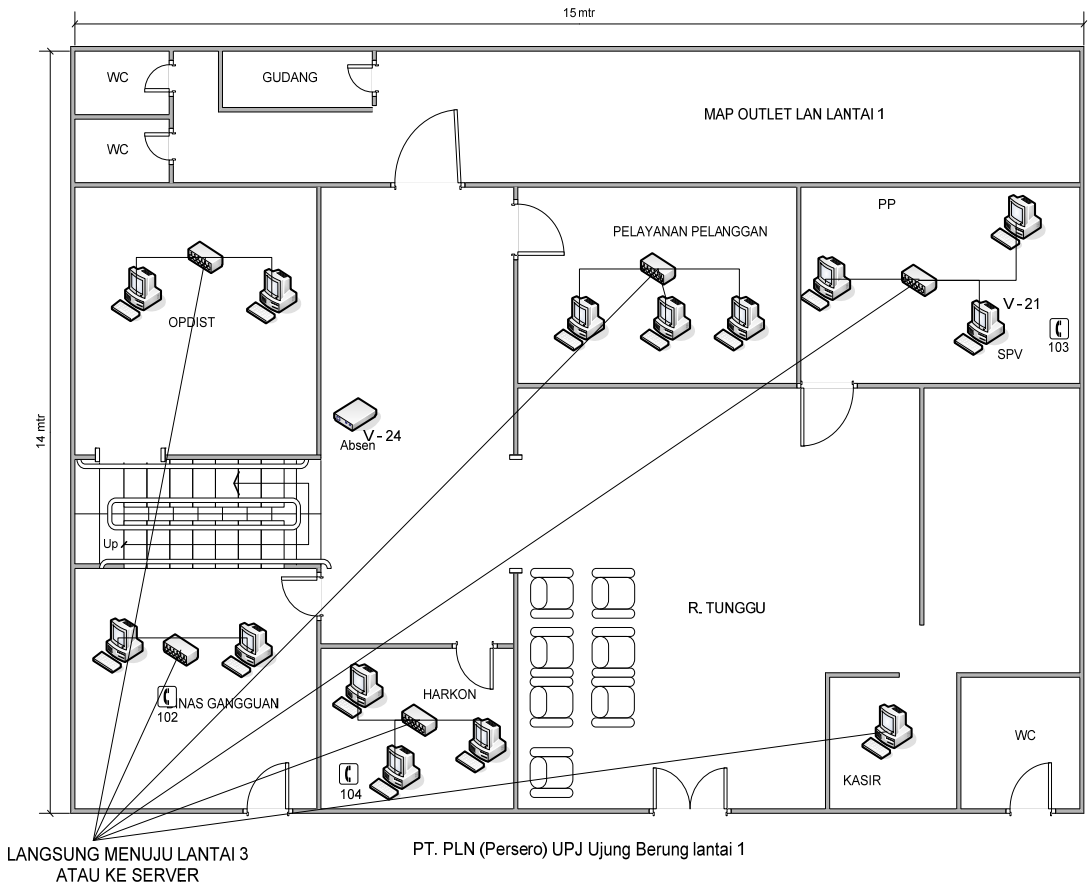
Sedangkan *host* atau *client* yang di miliki sekitar 55 host dengan mengunakan sistem operasi *Windows XP*, dengan spesifikasi *Hardware* yang berbeda-beda sesuai kebutuhan, dan semua terhubung dengan jaringan (LAN).

3.2.2.2 Topologi yang di gunakan

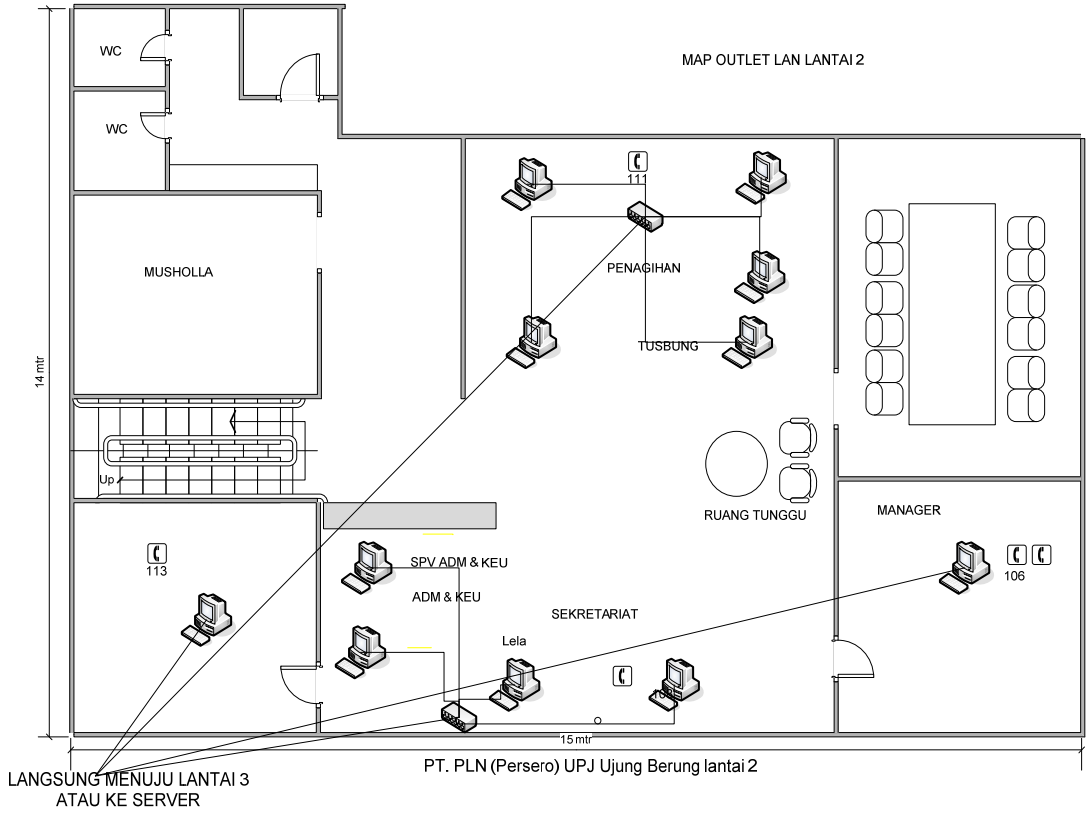
PT.PLN UPJ Ujung Berung menggunakan topologi *Star* untuk menghubungkan antar *host / client.*

Topologi ini memungkinkan setiap *node* terkoneksi ke pusat. Media transmisinya tertutup dan setiap client mempunyai kabel tersendiri untuk

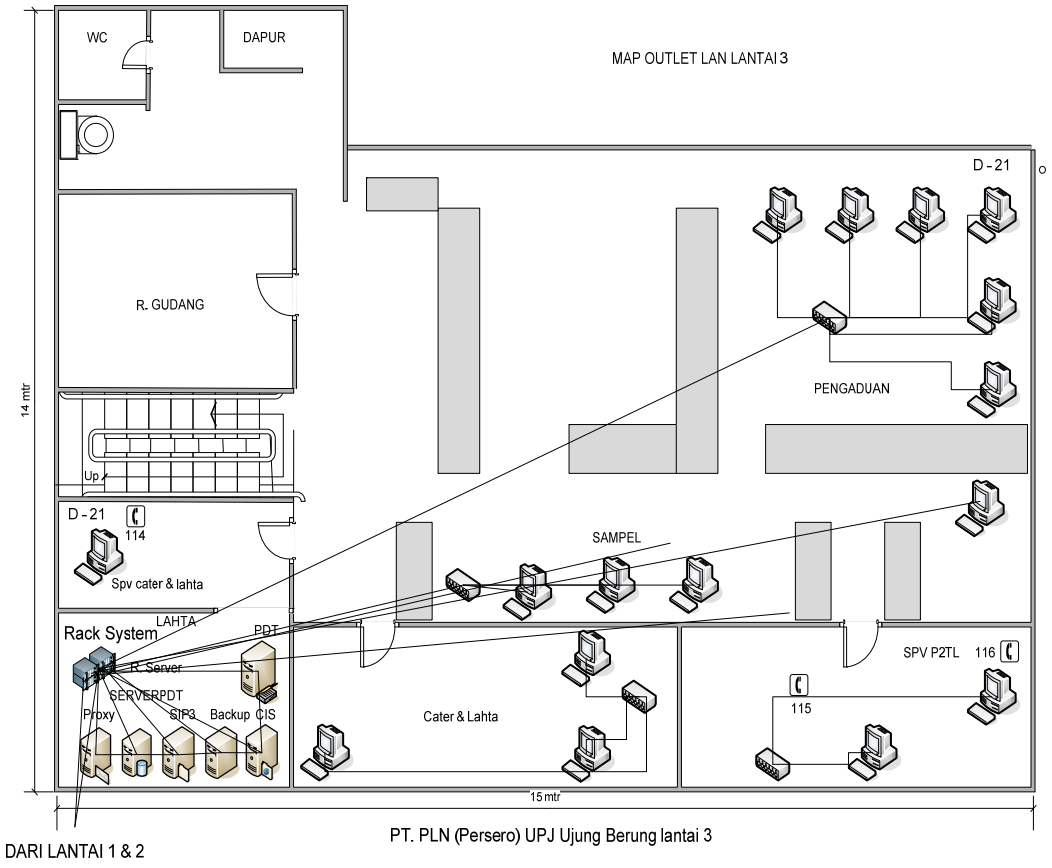
langsung berhubungan langsung dengan *file server*. Sehingga apabila salah satu *client* mengalami kegagalan, maka *client* yang lain tetap bisa berkomunikasi dengan *server*.. Kemudahan pemasangan dan sifatnya tetap bisa berkomunikasi dengan *server* walau pun ad salah satu yang rusak, dua hal ini yang menjadi sebagian alasan menganpa topologi *star* ini di pilihnya oleh perusahaan. Topologi ini juga sangat cocok dengan keadaan fisik di PT.PLN UPJ Ujung Berung yang berada dalam satu gedung yang terdiri dari tiga lantai, adapun *Layout* fisik jaringan loikal di PT.PLN UPJ Ujung Berung sebagai berikut:



Gambar 3. 1 Layout fisik LAN lantai 1



Gambar 3. 2 Layout fisik LAN lantai 2



Gambar 3. 3 Layout fisik LAN lantai 3

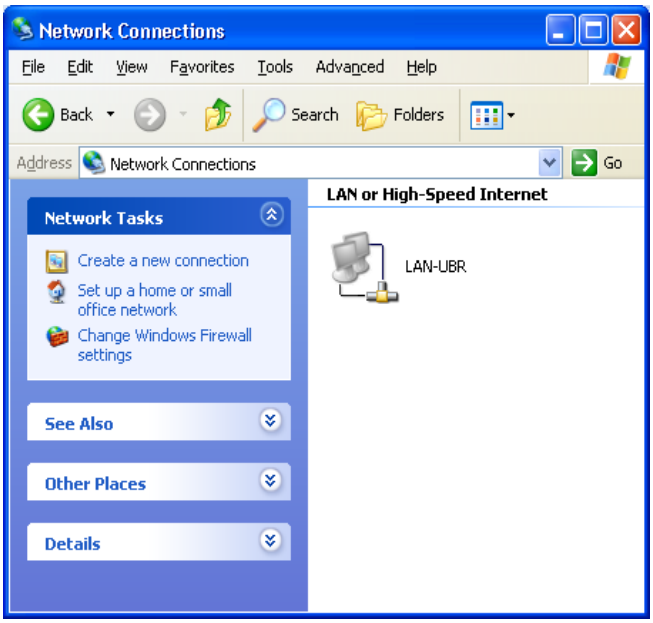
3.2.2.3 *IP Address*

IP address yang di gunakan adalah kelas A jaringan lokal di PT.PLN UPJ Ujung Berung . Penggunaan *IP address* kelas A sebenarnya kurang cocok untuk jaringan lokal di PT.PLN UPJ Ujung Berung karena hanya digunakan untuk lingkungan LAN saja.menggunakan kelas A berarti hanya ada 128 *network* yakni dari nomor 0.xxx.xxx.xxx sampai 127.xxx.xxx.xxx, tetapi setiap *network* dapat

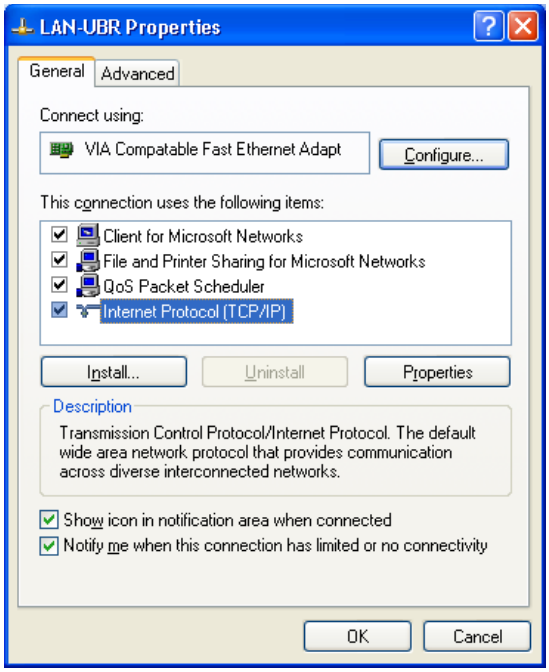
menampung lebih dari 16 juta (2563) host (xxx adalah variabel, nilainya dari 0 s/d 255). Ini jelas merupakan pemborosan alokasi *ip address*, jika hanya di gunakan untuk lingkungan LAN saja. Alokasi *ip address* yang pakai 10.2.23.1 - 10.2.23.254 *subnetmask* sebanyak 24 bit untuk jaringan LAN yaitu 10.2.23.0/24.

3.2.2.4 Konfigurasi IP pada Komputer

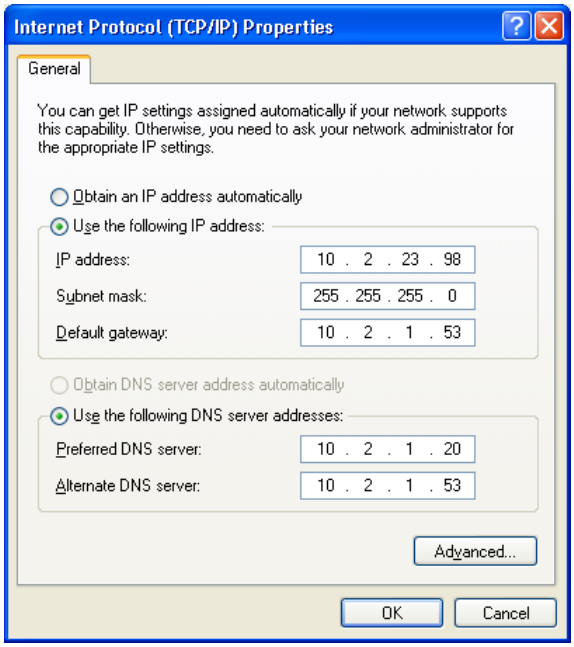
1. Start – Control Panel – Network Connection
2. Double klik Network connection
3. Pilih Local Area Connection – Klik kanan – Properties
4. Pilih Internet Protocol (TCP/IP) – Pilih Properties



Gambar 3. 4 Jendela Konfigurasi Koneksi Windows XP



Gambar 3. 5 Jendela Dialog Setting Protokol



Gambar 3. 6 Jendela Dialog Internet Protokol Properties

3.2.2.5 Pemakaian LAN di Perusahaan

LAN digunakan untuk menghubungkan kornputer yang berada di gedung perkantoran PT.PLN UPJ Ujung Berung Jarak antar komputer yang dihubungkannya relative dekat. Kecepatan mulai transmisi data yaitu 10 Mbps sampai 100 Mbps. LAN sangat cocok digunakan karena memungkinkan banyak pengguna untuk mernakai sumber daya secara. bersama-sama. Surnber daya yang biasa digunakan secara bersama-sama yaitu *file server* dan printer.

3.2.2.6 Keamanan pada LAN

Mengunakan *Firewall* dan antivirus menggunakan smadav dan smantek , *Firewall* di maksudkan untuk melindungan keamanan jaringan yang dimungkinkan adanya user (*hacker*) yang tidak bertanggung jawab masuk kesistem jaringan. Sedangkan untuk *antivirus server* adalah untuk mengamankan *server* dari serangan virus yang merupakan pintu utama dalam memberikan pelayanan kepada *client* baik data, program atau informasi lainnya.

3.2.4 Jaringan MAN di PT.PLN UPJ Ujung Berung

3.2.3.1. MAN yang berjalan

Metropolitan Area Network (MAN) yang menghubung kan antar UPJ-UPJ yang berada dalam satu kawasan APJ bandung, tercatat 10 gedung atau kantor yang terhubung dalam wan ini; diantaranya APJ Bandung, Kantor Distribusi, UPJ Ujungberung, UPJ Bandung selatan, UPJ Bandung timur,UPJ Bandung barat,UPJ Bandung utara,UPJ Kopo,UPJ Cijawura dan UPJ Priangan**.**

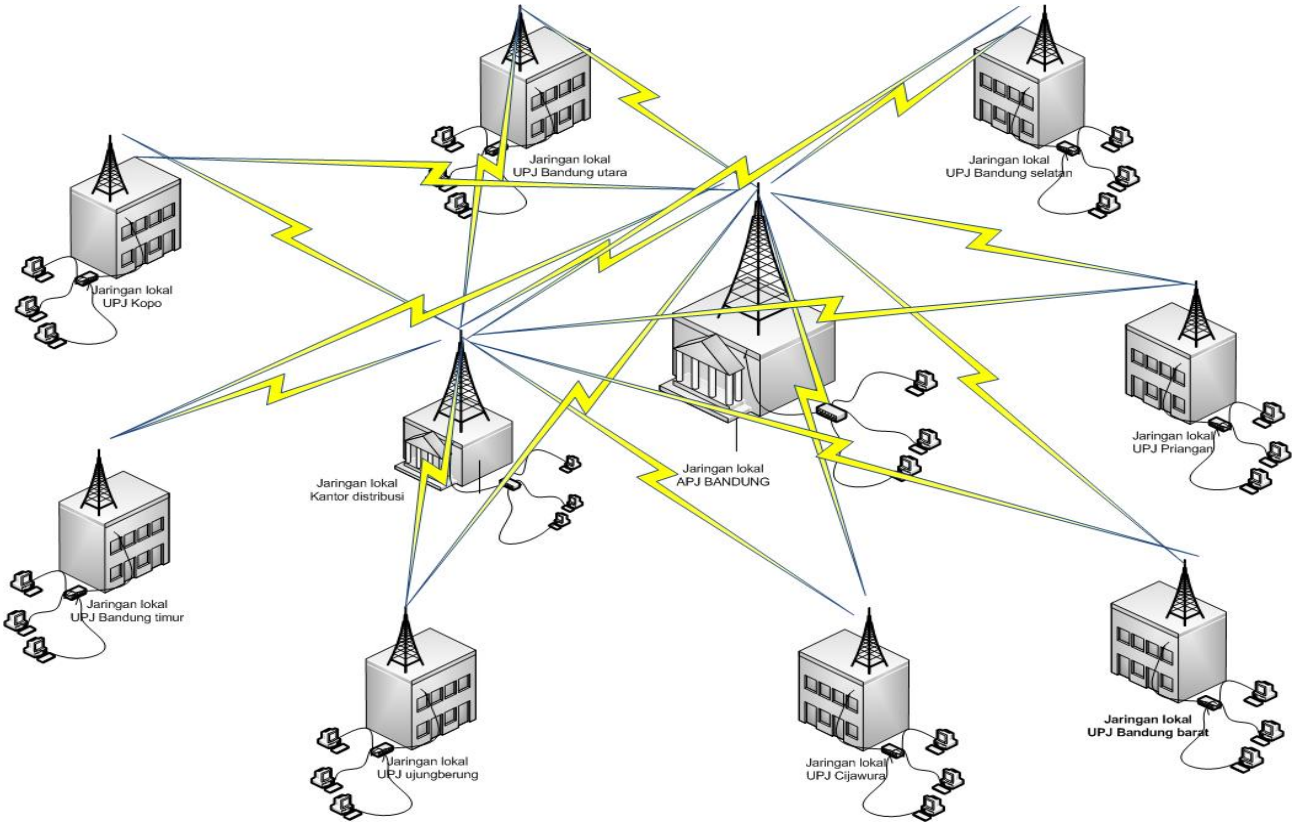
3.2.3.2. Pemakaian MAN

Adapun pemanfaatan man di UPJ Ujung Berung adalah untuk melakukan koneksi ke APJ bandung dan kantor distribusiini yang berguna untuk

a) *compare data base* dari apj atau pusat ke setiap UPJ
b) *sharing* data-data ter*update*
c) update aplikasi seperti *CM@X*
d) e-mail
e) *Sharing* data transaksi meliputi pelunasan,tunggakan data pembuatan baru,tambah daya dan lain-lain

3.2.3.3. Infrastuktur/ Skema MAN

Dalam MAN ini digunakan *Wireless* sebagai media interkoneksi *Local Area Network* (LAN) ketujuh gedung (UPJ Ujungberung, UPJ Bandung selatan, UPJ Bandung timur,UPJ Bandung barat,UPJ Bandung utara,UPJ Kopo,UPJ Cijawura dan UPJ Priangan). Tipe interkoneksi yang akan digunakan adalah ad-hoc (*point to point*) . Perangkat yang akan di gunakan adalah Wireless 10 Mbps. Ketujuh lokasi gedung tersebut interkoneksinya seperti digambarkan pada gambar dibawah ini.



Gambar 3. 7 Infrastuktur/ skema MAN

3.2.3.4. Keamanan pada MAN

Sistem keamanan yang di gunakan dalam MAN ini adalah *Network Firewall* , Pembangunan *Network Firewall* ini dimaksudkan untuk melindungan keamanan jaringan yang dimungkinkan adanya user (*hacker*) yang tidak bertanggung jawab masuk ke sistem jaringan PT.PLN APJ Bandung termasuk UPJ ujung berung di dalamnya, dan merusak atau mencuri data yang ada di dalam sistem jaringan tersebut. Dengan terpasangnya *firewall* maka user (*hacker*) yang akan masuk tanpa ijin akan di deteksi oleh sistem ini dan jika saat logon tidak memenuhi syarat maka akan ditolak oleh sistem ini.

3.2.4 Perangkat Keras *(Hardware)*

Perangkat yang digunakan untuk Jaringan diantaranya :

1. Media transmisi
    1. Kabel UTP
    2. Konektor RJ 45
2. Network Device
    1. Router 1 unit
    2. Layer 2 Fast Ethernet Switch
    3. Hub link 11 unit (4 hub di server dan 7 di client)
    4. Tower + alcatel
    5. Data Communication Rack, 1 unit

3.2.5 Perangkat Lunak *(Software)*

Perangkat Lunak yang digunakan di PT.PLN UPJ Ujung Berung meliputi perangkat lunak untuk server dan Sistem Operasi.

1. *Server*

    Menggunakan *windows 2000 server* dan *windows 2003 server* sebagai sistem operasinya.

    DBMS : ORACLE,

2. *Client*

    Menggunakan *Windows XP SP2* dan *XP3* sebagai sistem operasinya

    Microsoft Office 2003 Smadav Sebagai anti virus

3.2.6 Kendala-kendala yang sering dihadapi

Adapun kendala-kendala yang muncul setelelah melakukan analisa terhadap sistem jaringan yang ada di PT.PLN UPJ Ujung Berung yaitu ;

1. PC tidak bisa terkoneksi karena *hardware* jaringan yang rusak, hal ini tentu saja akan menjadi masalah pada sistem jaringan
2. Koneksi menjadi lambat dan pembagian koneksi internet yang tidak merata terlebih pada PC yang paling jauh dengan server karena terlalu panjang kabel yang menghubungkannya
3. PC tidak terkoneksi ke jaringan disebabkan terinfeksi virus jaringan. Virus yang sering di jumpai adalah Worm Win32/Conficker.A sering menyerang komputer client di jaringan yang memiliki celah keamanan RPC Dcom 3 yang belum di-patch. Jika berhasil, maka akan terdownload file virus ke komputer korban. Conficker dapat melumpuhkan System Restore dengan cara mereset "Restore Point" guna mencegah korbannya membasmi virus ini dengan mengembalikan Restore Point. Virus ini juga akan menyebabkan matinya Internet connection sharing. Gejala Conficker yang paling umum adalah munculnya pesan Generic Host Process Error setiap kali pengguna komputer menghubungkan dirinya dengan internet. Selain itu, Conficker juga diketahui menyebabkan login username Active Directory dikunci karena ia melakukan aksi Bruteforce.

3.2.7 Solusi atau Pemecahan Masalah

1. Solusi yang di sebabkan oleh rusaknya jaringan untuk mengetahuinya lakukan langkah-langkah sebagai berikut:
    a. *Pertama* dilihat kabelnya terlebih dahulu dicek menggunakan *LAN Tester*,
    b. Apabila keadaan kabel baik maka yang *kedua* adalah melihat *LAN Card* pada PC,
    c. Apabila sudah dicek dan keadaan *LAN Card* baik maka yang *ketiga* adalah melihat dari switch lalu dicek tiap port switch tersebut. Jika salah satu *deface* rusak maka akan diganti dengan *deface* yang lebih baik.
2. Untuk koneksi yang lambat dan pembagian akses internet yang tidak merata solusinya yaitu mengunakan Repeaters, sebagai penguat pengiriman paket data, atau dengan membagi 3 sub jaringan lokal perlantai dan menggunakan tambahan router. Menggunakan Router tambahan akan mengurangi beban trafik data pada router utama, sehingga dapat mempercepat aliran data.

3 PC tidak terkoneksi ke jaringan disebabkan terinfeksi virus jaringan.

Jika sudah dipastikan keadaan pada port baik, maka kemungkinan yang terjadi adalah serangan virus yang masuk ke dalam PC dan merusak sistem seperti menghilangkan salah satu *file* dalam sistem32 didalamnya, Serangan virus ini yang sering terjadi pada UBP Suralaya, maka untuk mendapatkan

data yang ada dalam komputer agar tidak hilang kendala ini dapat diatasi dengan cara:

A. Cara 1.

1. Terlebih dahulu masuk kedalam windows *safemode* lalu scan virus dengan antivirus yang ter-*up to date.*
2. Jika sudah bersih terhadap virus, untuk menghindari terjadinya kehilangan data, maka data pada PC di backup dengan menggunakan Program *backup* Media sebelum dilakukan *repair* windows,
3. Sesudah di *Backup* maka windows di*repair* ulang untuk me*repair* file yang hilang atau *corrupt*,
4. Jika ada aplikasi yang *corrupt* maka harus diinstal ulang kembali.
5. Apabila data yang telah di*backup* itu hilang karena proses *repair* maka tinggal di*restore* ulang dari *backup* yang telah dilakukan tadi.

B. Cara 2.

1. Dilakukan apabila cara 1 tidak dapat dilakukan (windows tidak membuka baik normal maupun *safemode*),
2. Lepas Hardisk, kemudian pasang di PC lain sebagai *slave*, kemudian lakukan *cleaning virus(scan),*
3. Lakukan sama seperti cara diatas (cara 1).

Jika antivirus pun masih gagal mengatasi, masih ada cara membasminya meski butuh sedikit kerja keras. Langkah-langkah membasmi virus Conficker dari Vaksincom berikut ini:

1. Putuskan komputer yang akan dibersihkan dari jaringan/internet. Matikan akses WiFi kalau ada dan cabut kabel ethernet dari jaringan LAN.
2. Matikan system restore (Windows XP/Vista). Caranya pilih Start>>All Program>>Accesories>>System Tools>>System Restore kemudian pada menu setting pilih off untuk seluruh partisi.
3. Matikan proses virus yang aktif pada services. Gunakan removal tool dari Norman untuk membersihkan virus yang aktif. Program ini tersedia dan dapat di*download* di http://norman.com/support/support_tools/58732/en-us
4. Delete service svchost.exe gadungan yang ditanamkan virus pada registry. Dapat dicari secara manual pada registry.
5. Hapus Schedule Task yang dibuat oleh virus. (C:-WINDOWS-Tasks)
6. Hapus string registry yang dibuat oleh virus. Untuk mempermudah dapat menggunakan script registry di bawah ini. Salin script ini lalu install.

```
[Version]

Signature=”$Chicago$”

Provider=Vaksincom Oyee

[DefaultInstall]

AddReg=UnhookRegKey

DelReg=del

[UnhookRegKey]

HKCU,          Software-Microsoft-Windows-
CurrentVersion-Explorer-Advanced,   Hidden,
0×00000001,1

HKCU,          Software-Microsoft-Windows-
CurrentVersion-Explorer-Advanced,
SuperHidden, 0×00000001,1

HKLM,          SOFTWARE-Microsoft-Windows-
CurrentVersion-Explorer-Advanced-Folder-
Hidden-SHOWALL, CheckedValue, 0×00000001,1

HKLM,    SYSTEM-CurrentControlSet-Services-
BITS, Start, 0×00000002,2
```

```
HKLM,    SYSTEM-CurrentControlSet-Services-
ERSvc, Start, 0×00000002,2

HKLM,    SYSTEM-CurrentControlSet-Services-
wscsvc, Start, 0×00000002,2

HKLM,    SYSTEM-CurrentControlSet-Services-
wuauserv, Start, 0×00000002,2

[del]

HKCU,          Software-Microsoft-Windows-
CurrentVersion-Applets, dl

HKCU,          Software-Microsoft-Windows-
CurrentVersion-Applets, ds

HKLM,          SOFTWARE-Microsoft-Windows-
CurrentVersion-Applets, dl

HKLM,          SOFTWARE-Microsoft-Windows-
CurrentVersion-Applets, ds

HKLM,    SYSTEM-CurrentControlSet-Services-
Tcpip-Parameters, TcpNumConnections
```

Gunakan notepad untuk menyalin, kemudian simpan dengan nama “repair.inf” (gunakan pilihan Save As Type menjadi All Files agar tidak terjadi kesalahan). Jalankan repair.inf dengan klik kanan, kemudian pilih install.

Catatan : Untuk file yang aktif pada startup, dapat men-*disable* melalui “msconfig” atau dapat men-*delete* secara manual pada string :

“`HKLM, SOFTWARE-Microsoft-Windows-CurrentVersion-Run`”

7. Untuk pembersihan virus W32/Conficker.DV secara optimal dan mencegah infeksi ulang, sebaiknya menggunakan antivirus yang ter-update dan mampu mendeteksi virus ini dengan baik dan patch komputer dengan masuk ke alamat web site www.microsoft.com/technet/security/Bulletin/MS08067mspx guna mencegah infeksi ulang.

Untuk mencegah virus ini menginfeksi lebih banyak komputer lakukan langkah berikut ini:

1. Pastikan virus tersebut tidak aktif di komputer. Caranya adalah dengan memutuskan hubungan komputer ke jaringan.

2. Jika setelah hubungan ke jaringan diputuskan infeksi virus terhenti, maka artinya sumber virus bukan dari komputer melainkan dari salah satu komputer di jaringan.
3. Cari sumber penyebar virus Conficker di jaringan sebelum mengkoneksikan komputer. Logikanya, semua komputer yang belum di-patch dan terhubung ke jaringan dimana ada satu komputer yang terinfeksi virus Conficker, maka akan terinfeksi Conficker juga dalam waktu singkat. Kecuali komputer-komputer tersebut dilindungi oleh Firewall yang memproteksi port:

    a. UDP Port 135, 137, 138 dan 445
    b. TCP Port 135, 139, 445 dan 593

4. Patch semua komputer yang sistem operasinya rentan terhadap celah keamanan RPC Dcom 3. Untuk mendapatkan detil *patch*-nya, dapat di*download* di situs Microsoft.

C. Cara 3

1. Instal ulang PC
2. Setelah di instal ulang gunakan antivirus yang kompatibel dan terupdate databasenya
3. Instalkan dan konfigurasi kembali program-program lain yang di butuhkan.