GUBERNUR DAERAH ISTIMEWA YOGYAKARTA

PERATURAN GUBERNUR DAERAH ISTIMEWA YOGYAKARTA
NOMOR 5 TAHUN 2006
TENTANG
PEDOMAN DAN PETUNJUK TEKNIS PEMANFAATAN JARINGAN KOMPUTER PEMERINTAH PROPINSI DAERAH ISTIMEWA YOGYAKARTA

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR DAERAH ISTIMEWA YOGYAKARTA,

Menimbang :

a. bahwa *Electronic Government* Pemerintah Propinsi Daerah Istimewa Yogyakarta terus dikembangkan untuk penyelenggaraan pemerintahan yang baik (*good governance*) dan meningkatkan pelayanan publik secara efektif dan efisien;

b. bahwa dalam rangka pengembangan *Electronic Government* Pemerintah Propinsi Daerah Istimewa Yogyakarta telah dibangun infrastruktur jaringan komputer yang menghubungkan instansi-instansi di lingkungan Pemerintah Propinsi Daerah Istimewa Yogyakarta;

c. bahwa untuk efektivitas dan efisiensi pemanfaatan jaringan *Electronic Government* Pemerintah Propinsi Daerah Istimewa Yogyakarta diperlukan pedoman dan petunjuk teknis pemanfaatan jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a, b, dan c perlu menetapkan Peraturan Gubernur Daerah Istimewa Yogyakarta tentang Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta.

Mengingat :

1. Undang-undang Nomor 3 Tahun 1950 tentang Pembentukan Daerah Istimewa Yogyakarta jo Peraturan Pemerintah Nomor 31 Tahun 1950 sebagaimana telah diubah dan ditambah terakhir dengan Undang-undang Nomor 26 Tahun 1959;

2. Undang-undang Nomor 10 Tahun 2004 tentang Pembentukan Peraturan Perundang-undangan;

3. Undang-undang Nomor 32 Tahun 2004 tentang Pemerintahan Daerah jo Undang-Undang Nomor 8 Tahun 2005

4. Undang-undang Nomor 33 Tahun 2004 tentang Perimbangan Keuangan antara Pemerintah Pusat dan Pemerintahan Daerah;

5. Peraturan Pemerintah Nomor 25 Tahun 2000 tentang Kewenangan Pemerintah dan Kewenangan Propinsi sebagai Daerah Otonom;

6. Keputusan Presiden Nomor 50 Tahun 2000 tentang Tim Koordinasi Telematika Indonesia;
7. Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *Electronic Government*;
8. Peraturan Daerah Propinsi Daerah Istimewa Yogyakarta Nomor 2 Tahun 2004 tentang Pembentukan dan Organisasi Lembaga Teknis Daerah di Lingkungan Pemerintah Propinsi Daerah Istimewa Yogyakarta;
9. Keputusan Gubernur Daerah Istimewa Yogyakarta Nomor 83 Tahun 2004 tentang Uraian Tugas dan Tatakerja Badan Informasi Daerah Propinsi Daerah Istimewa Yogyakarta.

MEMUTUSKAN:

Menetapkan : **PERATURAN GUBERNUR DAERAH ISTIMEWA YOGYAKARTA TENTANG PEDOMAN DAN PETUNJUK TEKNIS PEMANFAATAN JARINGAN KOMPUTER PEMERINTAH PROPINSI DAERAH ISTIMEWA YOGYAKARTA**

Pasal 1

Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta adalah acuan dalam optimalisasi pemanfaatan, pengelolaan, dan pemeliharaan jaringan komputer yang telah dibangun Pemerintah Propinsi Daerah Istimewa Yogyakarta.

Pasal 2

Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta sebagaimana tercantum dalam Lampiran Peraturan ini.

Pasal 3

(1) Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta sebagaimana tercantum dalam Lampiran Peraturan ini dapat ditinjau kembali dan disesuaikan dengan kemajuan teknologi informasi dan komunikasi yang berkembang di Propinsi Daerah Istimewa Yogyakarta.

(2) Perubahan Lampiran Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta sebagaimana tersebut pada ayat (1) , akan ditetapkan dengan Keputusan Sekretaris Daerah Propinsi Daerah Istimewa Yogyakarta.

Pasal 4

Peraturan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang dapat mengetahuinya, memerintahkan pengundangan Peraturan ini dengan penempatannya dalam Berita Daerah Propinsi Daerah Istimewa Yogyakarta.

Ditetapkan di Yogyakarta
pada tanggal 25 PEBRUARI 2006

GUBERNUR
DAERAH ISTIMEWA YOGYAKARTA,

HAMENGKU BUWONO X

Diundangkan di Yogyakarta
pada tanggal 25 PEBRUARI 2006

SEKRETARIS DAERAH
PROPINSI DAERAH ISTIMEWA
YOGYAKARTA

BAMBANG S. PRIYOHADI
NIP. 110 021 674

BERITA DAERAH PROPINSI DAERAH ISTIMEWA YOGYAKARTA
TAHUN 2006 **NOMOR** 5 **SERI** E

LAMPIRAN
PERATURAN GUBERNUR
DAERAH ISTIMEWA YOGYAKARTA
NOMOR 5 TAHUN 2006
TANGGAL 25 PEBRUARI 2006

PEDOMAN DAN PETUNJUK TEKNIS PEMANFAATAN JARINGAN KOMPUTER PEMERINTAH PROPINSI DAERAH ISTIMEWA YOGYAKARTA

I. PENDAHULUAN

A. Latar Belakang

Reformasi kepemerintahan di Indonesia telah melahirkan perubahan tatanan kehidupan bermasyarakat, berbangsa, dan bernegara. Tuntutan peningkatan kualitas dan pemerataan pelayan berkembang, meluas, dan menguat di kalangan masyarakat. Dalam kaitan ini, peran Aparatur Negara sebagai pelaksana penyelenggaraan negara dituntut untuk melakukan perubahan paradigma, strategi, dan metode dari regulasi menghambat *(wall regulation)* menuju regulasi mendorong *(enabling regulation)* untuk mewujudkan penyelenggaraan kepemerintahan yang baik *(good governance)*. Perwujudan *good governance* untuk tujuan peningkatan kualitas dan pemerataan pelayanan kepada masyarakat.

Perkembangan teknologi informasi dan komunikasi yang semakin pesat memungkinkan dibangunnya media yang mampu menjembatani berbagai muatan komunikasi. Pemanfaatan sistem jaringan komputer memungkinkan suatu instansi melakukan kegiatan administrasinya dengan lebih produktif, transparan, tertib, cepat, mudah, akurat, terpadu, aman, dan efisien, khususnya bagi kegiatan pemerintah sebagai fasilitator utama untuk memperlancar dan mendukung semua kegiatan pelayanan kepada semua pihak terkait *(stakeholders)*.

Dengan kemampuan teknologi informasi dan komunikasi ini melahirkan ide *Electronic Government* atau *E-Government* yakni manajemen pemerintahan, termasuk di dalamnya pelayanan, diselenggarakan menggunakan sarana dan media elektronik dengan komponen utama teknologi informasi dan komunikasi dalam bentuk sistem jaringan komputer. *E-Government* merupakan bagian dalam perwujudan penyelenggaraan kepemerintahan yang baik *(good governance)*. Dengan demikian pembangunan infrastruktur jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta merupakan salah satu jawaban untuk meningkatkan kinerja aparatur Pemerintah Propinsi Daerah Istimewa Yogyakarta. Infrastruktur jaringan komputer yang sudah ada harus dimanfaatkan seoptimal mungkin untuk peningkatan kualitas dan pemerataan pelayanan kepada masyarakat

Semua instansi pemerintah Propinsi Daerah Istimewa Yogyakarta termasuk Unit Pelaksana Teknis Daerah (UPTD) kecuali kantor UPTD yang lokasinya jauh dari jaringan komunikasi, telah diinterkoneksikan ke dalam jaringan komputer sehingga menjadi satu kesatuan sistem jaringan teknologi informasi dan komunikasi. Dengan terintegrasinya seluruh instansi Pemerintah Propinsi Daerah Istimewa Yogyakarta dalam satu jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta memungkinkan untuk menjalankan sistem pemerintahan dan pelayanan informasi yang efektif dan efisien, sehingga dapat meningkatkan kinerja aparatur dalam pelayanan kepada seluruh *stakeholders*-nya.

Dalam mengoptimalkan pemanfaatan jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta untuk meningkatkan kinerja, kualitas, dan pemerataan pelayanan semua instansi di Lingkungan Pemerintah Propinsi Daerah Istimewa

Yogyakarta diperlukan **Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta.**

B. Maksud dan Tujuan

1. Maksud

Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta dimaksudkan untuk digunakan sebagai acuan dalam pemanfaatan, pengelolaan, pemeliharaan, dan pengembangan Jaringan Komputer oleh seluruh Instansi Pemerintah Propinsi Daerah Istimewa Yogyakarta dalam rangka pelaksanaan *Electronic Government* Pemerintah Propinsi Daerah Istimewa Yogyakarta.

2. Tujuan

Tujuan dari diterbitkannya Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta adalah untuk mewujudkan keterarahan, optimalisasi dalam pemanfaatan, pengelolaan, pemeliharaan, dan pengembangan jaringan komputer oleh seluruh instansi Pemerintah Propinsi Daerah Istimewa Yogyakarta.

Adapun sasaran Pedoman dan Petunjuk Teknis Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta adalah untuk memberikan panduan kepada seluruh Instansi Pemerintah Propinsi *Daerah Istimewa Yogyakarta* agar dapat memanfaatkan, mengelola, memelihara, dan mengembangkan sistem jaringan komputer dengan baik guna mendukung tugas sehari-hari instansi yang bersangkutan.

C. Asas Pengembangan dan Pemanfaatan Jaringan Komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta, adalah :

1. Manfaat, pengembangan dan pemanfaatan jaringan komputer didasarkan pada nilai manfaat bagi seluruh pihak yang terkait *(stakeholders)*.
2. Produktivitas, pengembangan dan pemanfaatan jaringan komputer dilaksanakan dengan mempertimbangkan efisiensi biaya dan efektivitas dalam pengolahan data dan penyediaan informasi.
3. Keterbukaan, pengembangan dan pemanfaatan jaringan komputer untuk mendukung keterbukaan komunikasi.
4. Sinergisme, pengembangan dan pemanfaatan jaringan komputer dilaksanakan dengan saling memanfaatkan sistem lain yang telah ada untuk mengoptimalkan pemanfaatan jaringan.
5. Integrasi, pengembangan dan pemanfaatan jaringan komputer diorientasikan pada keterpaduan sistem guna mendukung pengambilan kebijakan Pemerintah Propinsi dan pelayanan informasi kepada masyarakat (publik) melalui sistem jaringan.
6. Standarisasi, pengembangan jaringan komputer harus dibuat standar yang meliputi:
   a. Kualifikasi perangkat keras;
   b. Kualifikasi perangkat lunak;
   c. Kualifikasi sumberdaya manusia.

D. Pengertian Teknis

1. Pemerintah Propinsi adalah Pemerintah Propinsi Daerah Istimewa Yogyakarta.
2. Badan Informasi Daerah (BID) adalah Badan Informasi Daerah Propinsi Daerah Istimewa Yogyakarta.
3. *Electronic Government (E-Government)* adalah penggunaan teknologi informasi dan komunikasi (telematika) untuk meningkatkan efisiensi, efektivitas, transparansi, dan akuntabilitas layanan pemerintahan.
4. Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer yang dapat digunakan untuk berkomunikasi (saling bertukar informasi).
5. Jaringan komputer internet adalah jaringan komputer yang saling terhubung dan menganut konsep terbuka, sehingga informasi yang ada di dalamnya dapat diakses secara luas.
6. Jaringan komputer intranet adalah suatu jaringan komputer yang menggunakan fasilitas *local area network (LAN)* atau *wide area network (WAN)* untuk keperluan internal.
7. Perangkat keras adalah sarana atau alat yang digunakan untuk komunikasi antar pihak dalam suatu sistem informasi manajemen dengan menggunakan jaringan komputer.
8. Perangkat lunak adalah sarana antarmuka untuk dapat berhubungan dengan komputer lain melalui jaringan sehingga pertukaran data dan pesan (dikirim dan diterima) antar komputer dapat terjadi dengan mudah.
9. Komputer *server* adalah suatu komputer dalam suatu jaringan yang berperan khusus memberikan pelayanan kepada komputer *client*.
10. Komputer *client* adalah sebuah komputer (biasanya berkemampuan lebih rendah) yang berperan sebagai pengguna dalam berinteraksi dengan komputer *server* (berkemampuan lebih tinggi) pada satu jaringan.
11. *Gateway* adalah perangkat keras yang mengarahkan paket data diantara fisik jaringan komputer yang berbeda. Langkah memilih *gateway* yang mana yang akan dipergunakan disebut membuat *routing*.
12. Media jaringan sarana utama penghubung titik dalam sistem jaringan komputer.
13. *Proxy Server* adalah perangkat lunak tambahan yang dipasang di dalam *server* yang bertindak sebagai perantara untuk menyimpan halaman-halaman *web* dalam yang diakses oleh pengguna sehingga apabila diperlukan bisa langsung ditampilkan tanpa harus benar-benar men-*download* dari komputer *server* penyimpan sehingga lebih cepat dan effektif.
14. *Hub* adalah perangkat yang memiliki banyak *port* yang akan menghubungkan beberapa titik atau *node* sehingga membentuk suatu jaringan pada *topologi star*. Pada jaringan yang umum dan sederhana salah satu *port* menghubungkan *hub* tersebut ke komputer *server*, *port* lainnya digunakan untuk menghubungkan komputer *client* atau *workstation* yang sudah memiliki *Network Interface Cart* (*NIC*) untuk membentuk suatu jaringan.
15. *Switch* adalah perangkat jaringan yang bekerja di lapisan *data-link* dan berfungsi menghubungkan banyak segmen *LAN* ke dalam satu jaringan yang lebih besar.
16. *Repeater* adalah perangkat keras atau *hardware* pada jaringan *topologi bus*. *Repeater* atau pengulang ini bekerja untuk memperkuat sinyal agar lalulintas data dari *client* ke *server* atau sebaliknya lebih cepat apabila jarak antara *client* ke *server* lebih jauh.

17. *Router* adalah sebuah perangkat berupa peralatan khusus atau komputer *PC* yang berfungsi untuk meneruskan paket-paket dari sebuah jaringan ke jaringan lainnya (baik *LAN* ke *LAN* atau *LAN* ke *WAN*) sehingga *host-host* yang ada pada sebuah jaringan bisa berkomunikasi dengan *host-host* yang ada pada jaringan yang lain.
18. *Compact Disk* yang selanjutnya disebut *CD* adalah piringan bundar yang terbuat dari logam atau plastik berlapis bahan yang bersifat magnet sebagai media penyimpan data elektronis;
19. *Flash Disk* atau *Universal Serial Bus* yang selanjutnya disebut *USB* adalah media magnetis kecil sebagai alat penyimpan data elektronis;
20. *IP Address* adalah alamat yang diberikan pada jaringan komputer dan peralatan jaringan yang menggunakan protokol *TCP/IP*. *IP Address* terdiri 32 bit angka *biner* yang dapat dituliskan sebagai empat kelompok angka desimal.
21. *Bastion Host* adalah bagian dari jaringan yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator atau dapat disebut bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen *firewall* atau bagian terluar sistem publik. Umumnya *Bastion host* akan menggunakan sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT).
22. Administrator adalah seorang atau beberapa orang yang mempunyai tugas untuk mengatur operator atau pengguna (*user*).
23. Pengguna (*user*) adalah seorang atau beberapa orang yang menggunakan jaringan komputer untuk akses data.
24. Sistem pengaman jaringan (*security system*) adalah sistem yang dibangun untuk mencegah pengaksesan secara tidak sah dan perusakan serta menjamin kerahasiaan data.

II. KEBIJAKAN DAN STRATEGI

A. Kebijakan

Dalam mengantisipasi dampak globalisasi yang ditandai meluasnya perkembangan infrastruktur informasi global yang difasilitasi oleh pesatnya kemajuan teknologi informasi dan komunikasi telah mengubah pola dan cara kegiatan ketatalaksanaan dalam pemerintahan. Kebijakan di bidang informasi dan komunikasi diarahkan pada pemanfaatan jaringan teknologi informasi dan komunikasi secara optimal sebagai dasar penerapan sistem informasi berbasis komputer untuk mendukung efektivitas dan efisiensi pengelolaan dan komunikasi data dan informasi antar instansi Pemerintah Propinsi Daerah Istimewa Yogyakarta.

Pemanfaatan jaringan komputer di lingkungan instansi Pemerintah Propinsi Daerah Istimewa Yogyakarta menjadi salah satu alat terselenggarakannya kepemerintahan yang baik *(good governance)* dan pemerintah yang bersih *(clean government)* dalam rangka meningkatkan transparansi dan akuntabilitas Pemerintah Propinsi Daerah Istimewa Yogyakarta, sehingga masyarakat mendapatkan pelayanan yang baik.

B. Strategi

1. Membangun, mengelola, dan mengembangkan jaringan komputer di lingkungan masing-masing instansi pemerintah dengan prinsip efisiensi dan efektivitas sumberdaya perankat keras teknologi informasi dan komunikasi.
2. Memanfaatkan sumberdaya perangkat keras dan perangkat lunak teknologi informasi dan komunikasi serta sumberdaya informasi sehingga dapat dilakukan penghematan biaya dan optimalisasi pemanfaatan.
3. Memanfaatkan jaringan komputer di lingkungan instansi sesuai dengan kebutuhan untuk mendukung sinergi dan peningkatan kinerja.
4. Memanfaatkan sumberdaya informasi untuk penggunaan bersama melalui jaringan komputer yang menkoneksikan antar instansi secara sinergis sehingga tidak terjadi tumpang tindih dan kontra produktif.
5. Mengadakan pendidikan dan pelatihan sistem jaringan komputer untuk memberdayakan dan meningkatkan kualitas sumberdaya manusia (SDM) di lingkungan Pemerintah Propinsi Daerah Istimewa Yogyakarta, serta membangun forum komunikasi antar instansi pemerintah dalam meningkatkan efektivitas jaringan komputer.

III. JARINGAN KOMPUTER

A. Definisi Jaringan Komputer

Jaringan komputer untuk mengartikan suatu himpunan *interkoneksi* sejumlah komputer yang *autonomous*. Dua buah komputer dikatakan terinterkoneksi bila keduanya dapat saling bertukar informasi. Betuk koneksinya tidak harus melalui kabel kawat tembaga, melainkan dapat menggunakan serat *optik*, gelombang mikro, atau satelit komunikasi.

B. Manfaat Jaringan Komputer

Ada beberapa manfaat jaringan komputer, yaitu :

a. ***Resource sharing*** bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh pengguna yang menggunakan jaringan tanpa terpengaruh lokasi resource dan pemakai. *Resource sharing* menghilangkan kendala jarak.

b. Jaringan komputer memberikan **reliabilitas tinggi** yaitu adanya alternatif perangkat pengganti jika terjadi masalah pada salah satu perangkat dalam jaringan, artinya adanya lebih dari satu perangkat dalam jaringan memungkinkan penggantian relatif cepat jika salah satu perangkat mengalami masalah.

c. **Skalabilitas** yaitu kemampuan untuk meningkatkan kinerja sistem secara bertahap sesuai beban pekerjaan dengan hanya menambahkan sejumlah prosesor.

d. Jaringan komputer mampu perpesan sebagai **media komunikasi** yang baik. Dengan menggunakan jaringan, dua orang atau lebih yang tinggal berjauhan akan lebih mudah bekerja sama dalam berbagai hal.

e. Dengan menggunakan internet dapat melakukan komunikasi dengan orang lain, fasilitas *electronic mail* (*email*) telah dipakai secara meluas oleh jutaan orang. Komunikasi menggunakan *email* ini masih mengandung *delay* atau waktu tunda. *Videoconference* atau pertemuan maya merupakan teknologi yang memungkinkan terjadinya komunikasi jarak jauh tanpa delay. Pertemuan maya ini dapat pula digunakan untuk keperluan sekolah jarak jauh, memperoleh hasil pemeriksaan medis seorang dokter yang berada di tempat yang jauh, dan sejumlah aplikasi lainnya.

f. *Video on demand* merupakan daya tarik ketiga jaringan komputer bagi orang per orang, sehingga dapat memilih film atau acara televisi dari negara mana saja dan kemudian ditampilkan di layar monitor.

C. Pengelolaan Jaringan

1. Pengembangan Jaringan

Pembangunan jaringan komputer lokal direncanakan dengan sistem kabel dan atau *wireless* dengan mempertimbangkan kondisi lingkungan. Selain itu pembangunan jaringan lokal komputer menggunakan topologi yang sesuai dengan kondisi ruangan dan kebutuhan.

a. Kriteria Umum

Secara umum, pengembangan jaringan sesuai dengan kriteria berikut :

1) Untuk membuat jaringan diperlukan minimal dua komputer dengan kelengkapan *network interface card* (*NIC*) yang masing-masing berfungsi sebagai *server* dan *client* (*workstation*).

2) Syarat *PC client* (*workstation*) untuk mengoperasionalkan jaringan harus mempunyai *network interface card* (*NIC*) minimal dengan prosesor pentium 4 (empat).

3) Setiap *node* (titik sambungan) dalam suatu kantor instansi pemerintah dapat disambung sampai dengan 30 *PC client (workstation).*

4) Media interkoneksi antar titik sambungan antar instansi menggunakan media kabel *hibrid fiber optic* (*HFC*) atau gelombang radio (*wave LAN*).

5) Media interkoneksi antar *client* (*workstation*) menggunakan kabel UTP atau gelombang radio.

b. Perangkat Keras Jaringan

Perangkat keras jaringan komputer ini meliputi:

1) Kabel modem;
2) *Router;*
3) *Server;*
4) *Hub/switch, repeater*;
5) *PC client (CPU, Key board, Monitor, Mouse);*
6) *Printer;*
7) *Firewall;*
8) *Proxy;*
9) Media jaringan.

c. Perangkat Lunak

1) *Server* komputer untuk jaringan menggunakan sistem operasi **Windows, Linux, Unix.**

2) Perangkat lunak *webserver* menggunakan ***Apache Server, Microsoft Internet Information Server (IIS), Personal Web Server (PWS), XITAMI, Netscape dan iPlanet servers, Oreilly Website Pro server, Caudium, OmniHTTPd,*** dan lainnya.

3) Perangkat lunak *mailsever* di Badan Informasi Daerah menggunakan ***Postfix Mail Server, Mdaemon.***

4) Perangkat lunak *database server* menggunakan ***Oracle, MySQL, Postgres, MS SQL***.

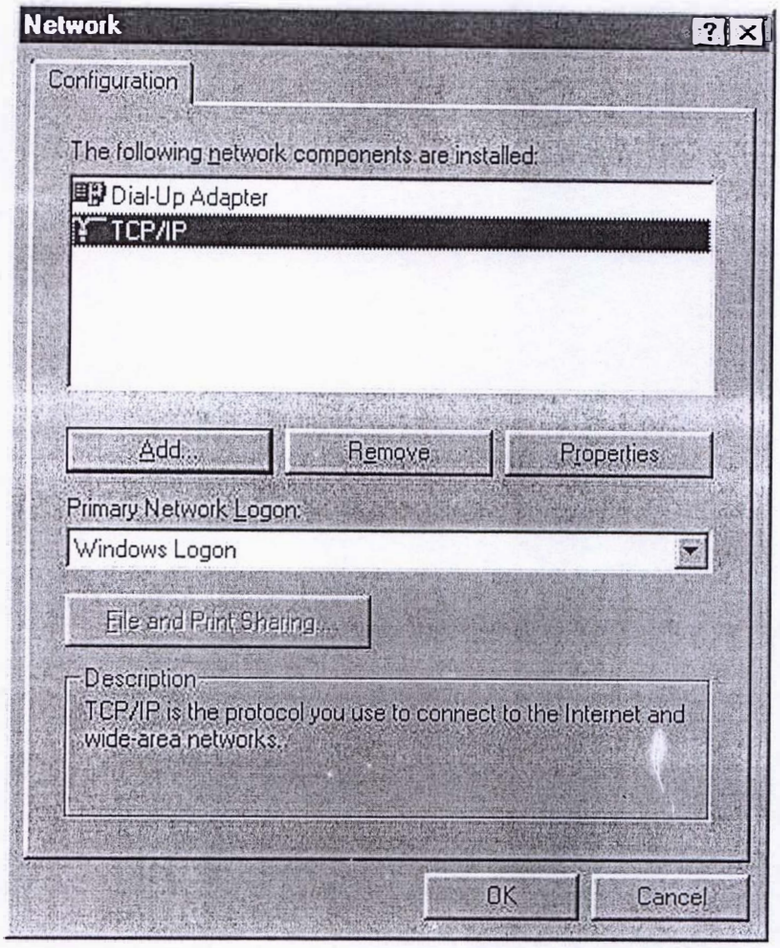
5) Masing-masing komputer *client* memerlukan perangkat lunak sistem operasi **Windows, Linux, Unix, Solaris**.

d. Protokol *TCP/IP*

Komunikasi antara dua komputer atau lebih memerlukan standarisasi atau protokol sebagai aturan-aturan/prosedur yang mengatur bagaimana dua sistem komputer saling berkomunikasi. *TCT/IP* (*Transmission Control Protocol/ Internetwork Protocol*) merupakan standar jaringan untuk berbagai *operating system*, dan merupakan protokol utama internet/intranet. Ada banyak protokol jaringan selain *TCP/IP* , antara lain : NetBEUI, NWLINK, IPX/SPX.

Cara Meng-*install* Protokol *TCP/IP*

Bila di ***Control Panel > Network,*** tidak terlihat adanya protokol *TCP/IP* ini, maka harus ditambahkan melalui menu :
Control Panel > Network > Add > Protokol > Microsoft > TCP/IP. Selanjutnya, sudah bisa dilihat protokol *TCP/IP* dari ***Control Panel > Network*** ini.



e. *IP Address*

IP Address adalah alamat yang diberikan pada jaringan komputer dan peralatan jaringan yang menggunakan protokol *TCP/IP* . *IP Address* terdiri 32 bit angka biner yang dapat dituliskan sebagai empat kelompok angka decimal. *IP Address* terdiri 2 bagian : *network ID* dan *Host ID*. *Network ID* menentukan alamat jaringan komputer sedangkan *Network ID* menentukan alamat *host* (komputer, *router, switch*).

IP Address dikelompokkan dalam IP Publik dan IP Privat. *IP Publik* adalah *IP Address* yang diberikan oleh lembaga internasional INTERNIC kepada publik. *IP* ini dipakai pada jaringan yang berhubungan langsung dengan internet. *IP Privat* adalah *IP address* yang disediakan untuk pemakai pada jaringan *LAN* yang tidak terhubung langsung dengan internet.

2. Pengelolaan Jaringan

a. Pemanfaatan jaringan harus selalu mempertimbangkan kebersihan dan ketertiban. Untuk itu harus memperhatikan hal-hal berikut :

1) Setiap pengguna perangkat jaringan komputer dilarang untuk meng-*install* program aplikasi baru atau menghapus program aplikasi yang telah ada, kecuali ada ijin dari administrator jaringan.

2) Setiap pengguna dilarang mengganti *IP* komputer dalam jaringan lokal untuk menghindari terjadinya konflik *IP* antar komputer dalam jaringan lokal yang sama.

3) Dalam berkomunikasi memanfaatkan perangkat jaringan komputer Propinsi Daerah Istimewa Yogyakarta harus menjaga sopan santun berkomunikasi.

4) Para pengguna wajib menjaga kebersihan peralatan komputer dan dilarang meletakkan makanan, minuman dan benda cair lainnya, serta merokok di depan komputer.

b. Untuk menjaga agar jaringan tetap dapat berfungsi sebagaimana mestinya, secara teknis jaringan harus selalu dipantau dan dipelihara. Hal-hal yang perlu dilakukan adalah sebagai berikut.

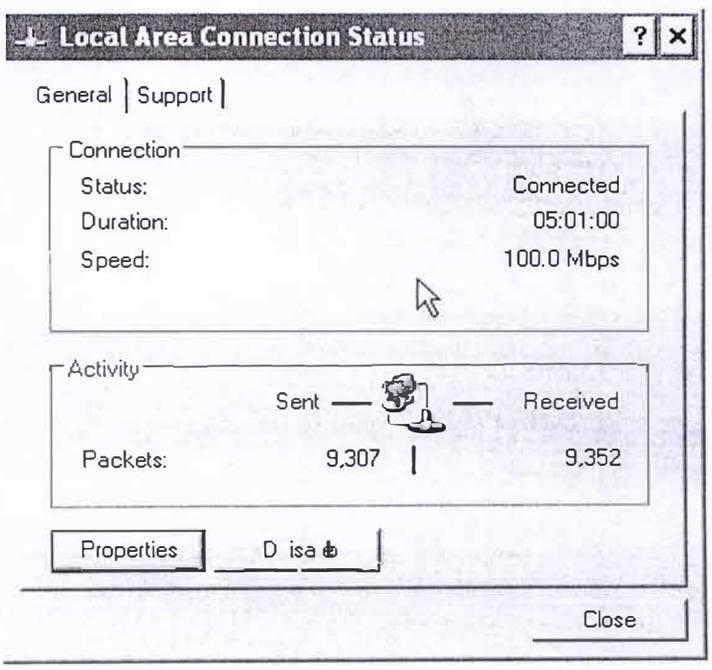
1) ***Setting IP***

Setting IP untuk komputer dalam jaringan lokal yang tehubung dengan internet dilakukan sedemikian rupa sehingga masing-masing mempunyai *IP* yang unik. Untuk itu *setting* dilakukan dengan melihat *IP* jaringan lokal yang telah ditentukan. Kesalahan *setting IP* berakibat komputer yang bersangkutan tidak dapat mengakses jaringan. Kesalahan *Setting IP* dapat berupa ketidaksesuaian dengan *IP* jaringan maupun *IP* ganda (tidak unik).

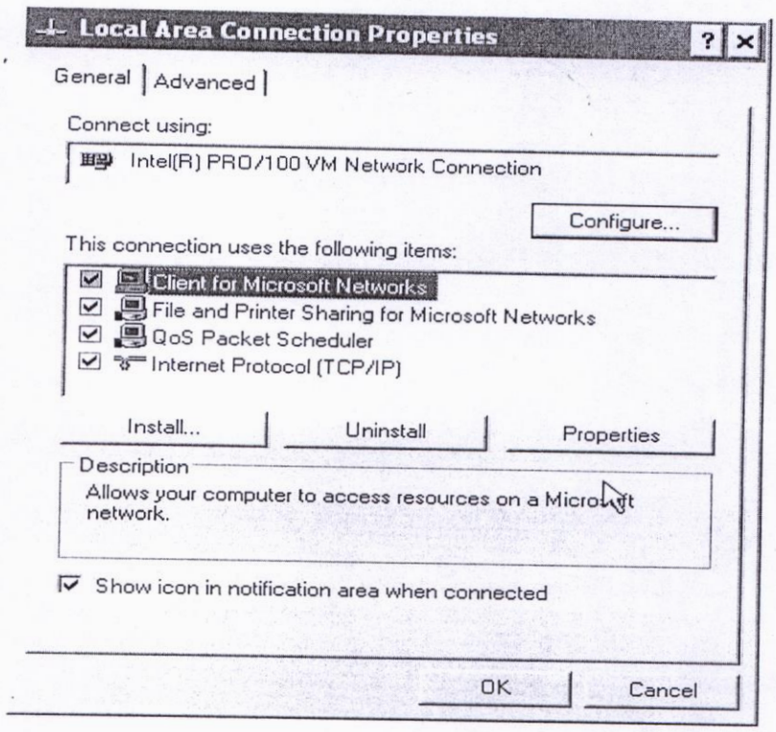
Untuk menjaga kelancaran kinerja jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta, *setting IP* komputer masing-masing instansi yang telah tersambung dengan jaringan yang dikelola oleh Badan Informasi Daerah (BID) Propinsi Daerah Istimewa Yogyakarta.

Adapun cara untuk *setting* IP pada komputer (untuk Windows XP) adalah sebagai berikut.

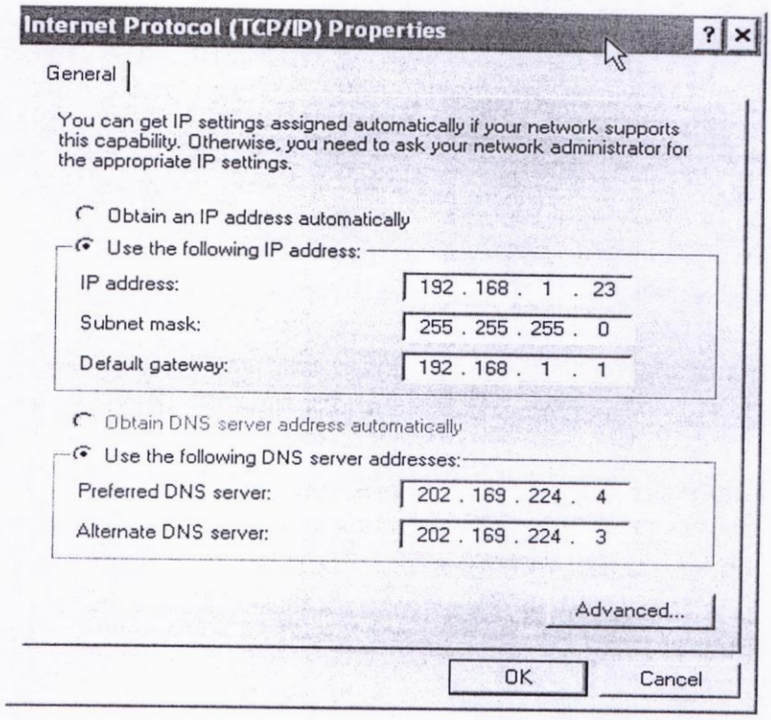
a) Klik ***Local Area Connection***



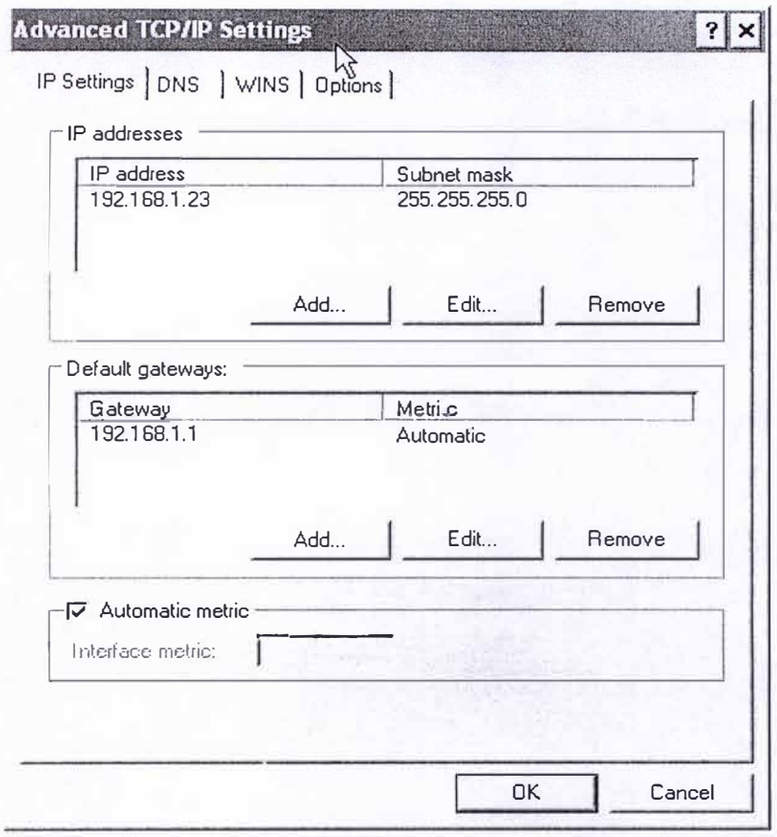
b) Klik ***Properties.***



c) Klik ***Internet Protocol (TCP/IP) >Properties.***



d) Klik ***Advanced.***



e) Klik ***OK.***

2) Memeriksa dan mengetahui ***IP Address***, dengan cara:
   a) Klik ***Start*** > ***Run.***
   b) Ketik ***cmd*** > ***tekap Enter*** (atau klik ***OK***).
   c) Ketikkan : ***ipconfig.***

3) Melakukan **test koneksi jaringan**
   a) Klik ***Start*** > ***Run.***
   b) Ketik ***cmd*** > ***tekan Enter*** (atau klik ***OK***).
   c) Ketikkan : ***ping*** *IP Address* (contoh : *ping* 192.168.1.23).

4) Mengetahui **nama komputer**
   a) Klik ***Start*** > ***Run.***
   b) Ketik ***cmd*** > ***tekap Enter*** (atau klik ***OK***).
   c) Ketikkan : ***net config.***

3. Sumberdaya Manusia (SDM)

a) Kebutuhan SDM

1) Untuk membangun, mengelola, dan mengembangkan jaringan komputer diperlukan SDM yang mempunyai spesialisasi keahlian di bidang teknisi komputer dan teknisi jaringan.

2) Teknisi komputer adalah orang yang mempunyai keahlian dalam merakit, men-*setting*, dan memperbaiki komputer.

3) Teknisi jaringan adalah orang yang mempunyai keahlian dalam merencanakan, men-*setting*, dan memperbaiki jaringan komputer sedemikian rupa jaringan dapat beroperasi dengan baik dan aman dari gangguan pengguna komputer yang tidak berhak.

b) Kebutuhan Pelatihan SDM

1) Untuk menyiapkan SDM yang mempunyai spesialisasi keahlian membangun, mengelola, dan mengembangkan jaringan komputer diperlukan pelatihan teknisi komputer, teknisi jaringan, dan keamanan jaringan komputer.

2) Pelatihan teknisi komputer adalah pelatihan teknis perakitan, *setting*, dan perbaikan kinerja sistem komputer.

3) Pelatihan teknisi jaringan dan keamanan jaringan komputer adalah pelatihan teknis perencanaan, pemasangan, *setting*, dan pemeliharaan jaringan komputer.

V. PEMANFAATAN JARINGAN

Dalam rangka menunjang kegiatan pemerintahan dan pelayanan masyarakat di lingkungan Propinsi Daerah Istimewa Yogyakarta, pemanfaatan sistem jaringan komputer ditujukan untuk :

1. Pemberdayaan peralatan Perangkat keras (*hardware*).
2. Pemanfaatan dengan bagi-pakai Dokumen/File (*file sharing*).
3. Komunikasi.

A. Pemberdayaan peralatan *hardware*

Komputer-komputer *PC* lama yang masih baik dapat dimanfaatkan untuk menambah fungsionalitas pekerjaan komputasi yang kebanyakan tidak memerlukan mesin canggih. Hampir semua *PC* lama mampu bertindak sebagai *server file* jaringan, *print server* jaringan, atau *sharing point* untuk koneksi Internet. Sebuah sistem berbasis Pentium 133MHz dengan *RAM* 32MB atau 64MB masih mampu melakukan tugas-tugas dasar jaringan. Windows 98 SE dan Windows Me memiliki kemampuan *sharing* yang terintegrasi, hanya perlu mengaktifkannya.

Beberapa langkah yang perlu dilakukan terhadap *PC* Lama :

- Buang program yang tidak diperlukan. Jika *PC* lama dalam jaringan tidak akan menjalankan macam-macam aplikasi, *setting* dengan : ***Start > Settings > Control Panel,*** dan klik-dua kali ***Add/Remove Programs (Start > Control Panel > Add or Remove Programs*** di Windows XP). *Uninstall* semua program yang tidak akan digunakan. Setelah selesai, gunakan **Windows Explorer** untuk memeriksa direktori **Program Files**, apakah masih ada file-file data yang tidak diperlukan.
- Bersihkan drive. Kebanyakan *hard drive* berisi sejumlah besar *browser cache* dan *temporary files*.
- Pasang kartu jaringan apabila komputer lama tidak punya *adapter* jaringan (kecuali *PC* lama tersebut hanya akan digunakan sebagai *PC stand-alone*).

a). *Server File* Jaringan

Untuk dijadikan *Server* File Jaringan, *PC* lama harus mempunyai kualifikasi :

Prosesor	: Pentium 133 ke atas
RAM	: 32MB atau ke atas
Harddisk	: 10GB atau ke atas
Sistem operasi	: Windows 98 ke atas
kartu jaringan	: Harus ada

PC jaringan yang digunakan untuk menyimpan file-file tidak memerlukan banyak tenaga. Jika *hard drive* di *PC* tua besarnya 20GB atau lebih, memiliki cukup ruang untuk pekerjaan dasar file *sharing* dan *backup*. Namun jika ingin menyimpan banyak file, membuat *backup* besar, atau berbagi-pakai media digital (file-file gambar, suara, video), mungkin perlu memasang *harddisk* kedua yang kapasitasnya lebih besar. Adapun caranya adalah sebagai berikut :

1) **Aktifkan *file sharing***. Klik-kanan ***Network Neighborhood*** (Windows 98) atau ***My Network Places*** (Windows Me, Windows 2000, atau Windows XP), dan pilih **Properties**. Pada Windows 98 atau Windows Me, klik ***File and Print Sharing***, beri tanda *check* ***I want to be able to give others access to my files***, dan klik ***OK***. Pada Windows 2000 atau Windows XP, klik-kanan ***Local Area Connection***, pilih ***Properties***, dan beri tanda *check* pada ***File and Printer Sharing for Microsoft Networks***. Kemudian *restart PC*.

2) Bagi-pakai (*sharing*) drive. Klik-dua kali ***My Computer***, klik-kanan *icon* untuk ***drive*** atau ***folder*** yang ingin dibagi-pakai, dan pilih ***Sharing***. Ikuti petunjuk di layar untuk men-*setup sharing*. Pilihan yang bisa dilakukan adalah ***full access***, ***read-only access***, atau ***password-based access***. Ulangi proses tersebut untuk drive lainnya.

b). *Server Print* Jaringan

Untuk dijadikan *Server* Print Jaringan, *PC* lama harus mempunyai kualifikasi :

Prosesor	: Pentium 133 ke atas
RAM	: 32MB atau ke atas
Harddisk	: 1GB atau ke atas
Sistem operasi	: Windows 98 ke atas
Peralatan Lain	: Kartu jaringan, Printer

Dengan *print server* mempermudah berbagi-pakai sebuah *printer* (*printer sharing*), dan untuk ini *PC* lama bisa digunakan sebagai *print server*. Adapun caranya adalah sebagai berikut :

a. Pasang *printer*. Ikuti petunjuk manufaktur *printer* untuk menghubungkan *printer* dan meng-*install* driver untuknya.

b. Aktifkan bagi-pakai *printer*. Ikuti instruksi seperti seting ***Server File* Jaringan** untuk mengaktifkan bagi-pakai file. Pada Windows 98 dan Windows Me, juga beri tanda *check* ***I want to be able to allow others to print to my printer(s)*** pada kotak dialog di Langkah pertama (1) proyek di atas. Kemudian *restart PC*.

c. Bagi-pakai *printer*. Pada Windows 98, Windows Me, atau Windows 2000, pilih ***Start > Settings > Printers***; di Windows XP, pilih ***Start > Printers and Faxes***. Klik-kanan *icon printer* yang ingin dibagi-pakai, dan pilih ***Sharing***. Ikuti petunjuk di layar. Selanjutnya bisa menyetel permintaan *password* untuk mengakses *printer*.

c). *Internet Connection Sharing Point*

Untuk dijadikan *Internet Connection Sharing Point*, *PC* lama harus mempunyai kualifikasi :

Prosesor	: Pentium 266 ke atas
RAM	: 64MB atau ke atas
Harddisk	: 5GB atau ke atas
Sistem operasi	: Windows 98 SE ke atas
Peralatan Lain	: Modem, Kartu jaringan kedua, atau *port USB*

1) Jika menggunakan koneksi *dial-up* Internet perlu pasang *modem* atau kartu jaringan, jika menggunakan koneksi *broadband*, memerlukan kartu jaringan agar terkoneksi ke jaringan lokal. Dan akan perlu kartu jaringan kedua untuk *modem cable* atau DSL, kecuali memiliki *modem broadband USB*.
2) *Install* ***Internet Connection Sharing***. Pada Windows 98 atau Windows Me, buka ***Add/Remove Programs*** *di* ***Control Panel***, dan pilih *tab* ***Windows Setup***. Klik-dua kali ***Internet Tools*** (Windows 98) atau ***Communications*** (Windows Me). Beri tanda *check* ***Internet Connection Sharing***, klik ***OK***, dan jalankan

Internet Connection Sharing Wizard atau ***Home Networking Wizard***. Di Windows 2000 atau Windows XP, klik-kanan ***My Network Places***, pilih ***Properties***, klik-kanan **koneksi** ***modem broadband***, dan pilih ***Properties***. Di Windows 2000, klik *tab* ***Sharing***, dan beri tanda *check* ***Enable Internet Connection Sharing for this connection***. Di Windows XP, klik *tab* ***Advanced***, dan pilih ***Allow other network users to connect through this computer's Internet connection.***

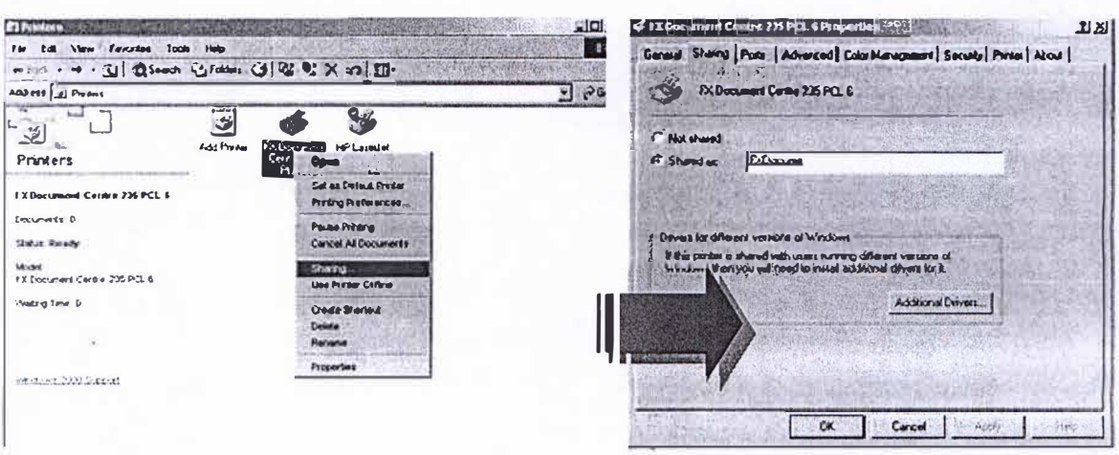
B. Pemanfaatan dengan bagi-pakai Peralatan Printer (*printer sharing*) dan Dokumen/File (*file sharing*)

Dengan jaringan sistem komputer, berbagai dokumen elektronik (file) dapat digunakan bersama oleh beberapa pengguna. Hal ini sangat mendukung efisiensi pekerjaan.

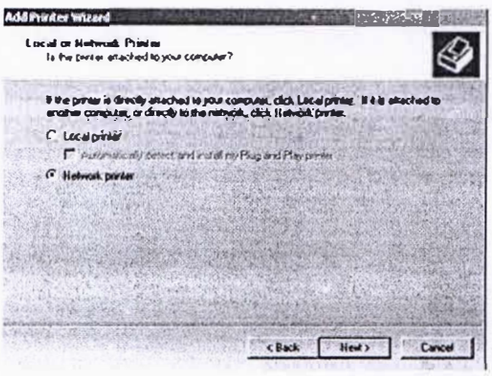
1. *Printer Sharing*

Dengan menggunakan jaringan *LAN*, beberapa komputer bisa memanfaatkan sebuah *printer* bersama-sama. Dengan satu komputer yang terkoneksi ke *printer*, dan men-*share printer* tersebut agar bisa digunakan oleh komputer lainnya.

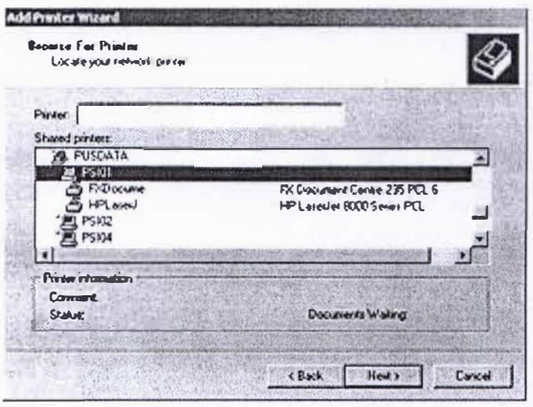
1) Jaringan komputer dapat dimanfaatkan untuk mengoptimalkan penggunaan peralatan *printer*.
2) Satu *printer* dapat dimanfaatkan oleh lebih dari satu komputer secara besama-sama (*printer sharing*).
3) Cara *setting* untuk *printer sharing* adalah :
   - Pada komputer yang terkoneksi pada *printer* dan mengasumsikan driver *printer* tersebut telah ter-*install*, klik ***Start > Settings > Printers*** untuk menampilkan nama *printer* yang ada pada komputer.
   - Klik kanan pada *icon printer* yang hendak di-*share* dan klik ***Sharing***...



- Untuk men-*share* nama *printer* berikan dengan nama lain atau nama *default*-nya pada kolom ***Shared as*** : dan klik ***OK***. *Printer* telah di-*share* ke jaringan dengan ditandai adanya gambar tangan pada *icon printer* yang telah di-*share*. Pada komputer lain, untuk bisa mengakses *printer* yang di *share*, klik ***Start > Settings > Printers > Add Printer***.
- Pada tampilan ***Welcome to the Add Printer Wizard*** klik ***Next***. Kemudian pada tampilan seperti di bawah ini, pilih ***Network Printer*** dan klik ***Next***.



- Saat ditanya nama *printer* yang akan diakses, klik ***Next*** agar bisa langsung mem-browse *printer* tersebut, untuk mencari tahu nama *printer* yang di-*share*.
- Pilih nama ***groups***, double-klik nama komputer tempat *printer* itu di-*share*. Akan muncul nama *printer* tersebut persis di bawah komputer yang men-*share printer*. Sorot nama *printer* dan klik ***Next***.



- Pada pilihan untuk menjadikan *printer* tersebut default atau tidak, sepenuhnya tergantung pilihan pengguna. Klik ***Next***, dan setelah selesai, klik ***Finish***. Komputer *user* sudah bisa menggunakan *printer* tersebut untuk mencetak seolah-olah mencetak pada *printer* sendiri.

Memeriksa *Crash*

- Klik kanan ***My Computer***, pilih ***Properties***.
- Klik pada *tab* ***Device Manager***.
- *Device Manager* akan menampilkan daftar *driver* yang di-*install*. Apabila terdapat tanda (!) atau (x), berarti ada masalah.

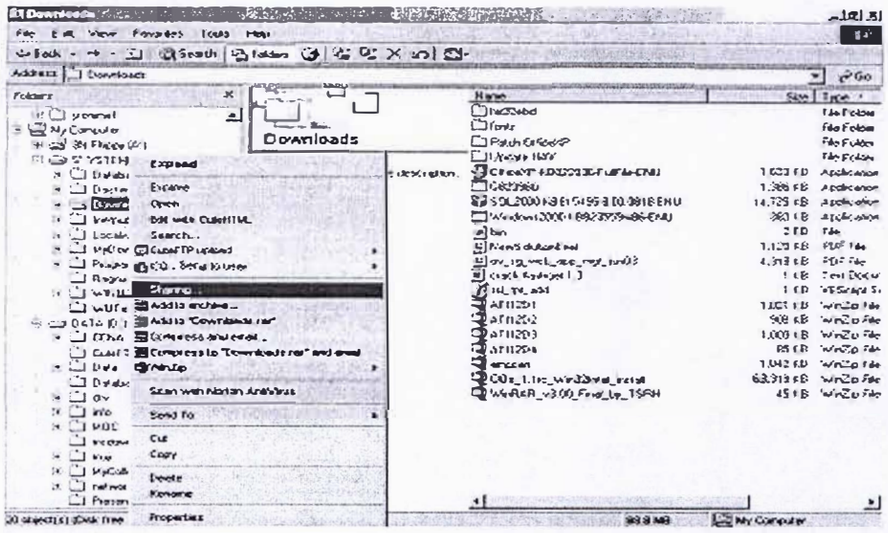
2. Folder dan File sharing

File-file yang ingin di *share* harus terlebih dahulu dimasukkan ke dalam suatu *folder* yang di-*share*.

1) File Sharing adalah pemanfaatan dokumen elektronis (file) secara bersama-sama oleh berbagai *user*.
2) File-file disimpan dalam komputer tertentu yang dapat diakses oleh berbagai *user*.
3) File-file berupa *database*, data teks, data gambar (grafis), maupun data suara.

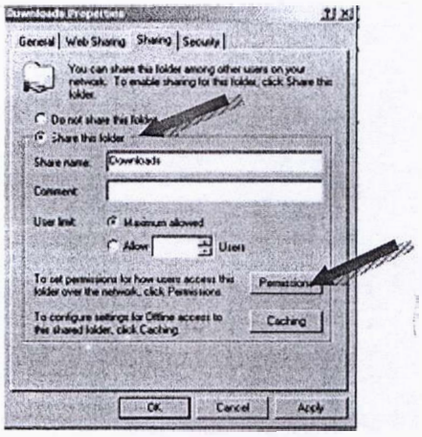
Adapun cara men-*setting Folder* dan *File sharing* adalah sebagai berikut:

1) Pada tampilan ***Windows Explorer***, klik kanan *folder* yang akan di-*share* dan klik ***sharing***.



2) Pilihan sharing apabila di komputer tersebut telah di-*install* ***File and Printer Sharing for Microsoft Networks***. Fitur ini sudah standar pada versi Windows 2000 Pro dan Windows XP Pro. Untuk versi lain, fitur tersebut harus di-*install* terlebih dahulu dengan menggunakan *CD* Instalasi Windows.

3) Klik pada pilihan ***Share this folder*** . Pemilik *folder* juga bisa menentukan pilihan-pilihan lain seperti nama *share* yang ditampilkan (bila ingin beda dengan nama *folder* aslinya) serta jumlah akses yang boleh membukanya bersamaan.



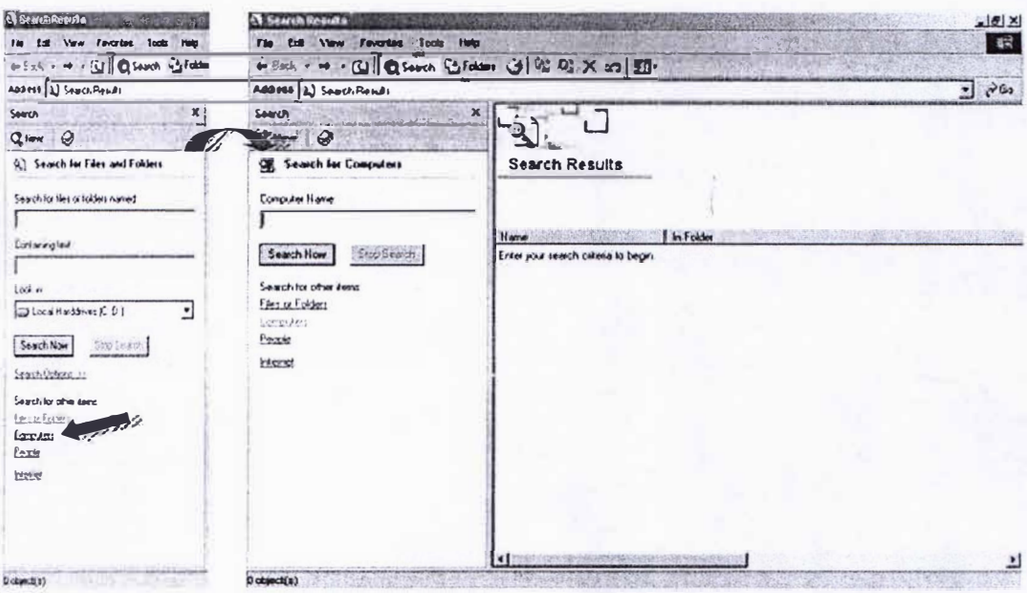
4) Gambar di atas adalah tampilan yang muncul pada versi Windows 2000 dan tidak jauh berbeda dengan Windows XP. Untuk keamanan, *user* bisa memilih men-*share* ***folder*** tersebut kepada orang-orang tertentu yang memiliki ***User ID*** dan ***password*** pada komputer tersebut dengan meng-klik ***permission.***

5) Untuk versi Windows 98, tampilan yang muncul lebih sederhana. *User* langsung menentukan *password* yang harus digunakan untuk membuka *folder* tersebut.

Cara mengakses *folder* yang di-*share* pada komputer lain :

1) Untuk bisa mengakses *folder* yang disharing oleh komputer lain, harus terlebih dahulu mengetahui nama komputer di mana *folder* tersebut berada. Cara paling cepat menemukan komputer target adalah dengan mencarinya dari menu ***Search / Find***.
2) Klik ***Start>Find>Computer*** untuk Windows 98 dan ketikkan nama komputer yang ingin dicari.

Untuk Windows 2000 dan Windows XP, klik ***Start>Search>For Files or Folders***... dan kemudian pilih untuk ***Computer*** dan tampilan akan berubah seperti gambar di bawah sebelah kanan.



3) Ketikkan nama komputer yang dicari dan klik ***Search Now***. Bila nama komputer yang dimasukkan benar dan komputer yang dimaksud dihidupkan dan terkoneksi ke jaringan, maka nama komputer tersebut akan muncul di layar sebelah kanan. Klik ganda nama komputer tersebut dan akan muncul deretan *folder* yang di-*share* pada komputer tersebut.
4) Bila diminta oleh pemilik *folder*, maka perlu diberikan ***User ID*** dan ***password*** yang benar sebelum bisa mengakses file-file di dalam *folder sharing* tersebut.

C. Untuk Komunikasi

1. Untuk Mengakses Internet

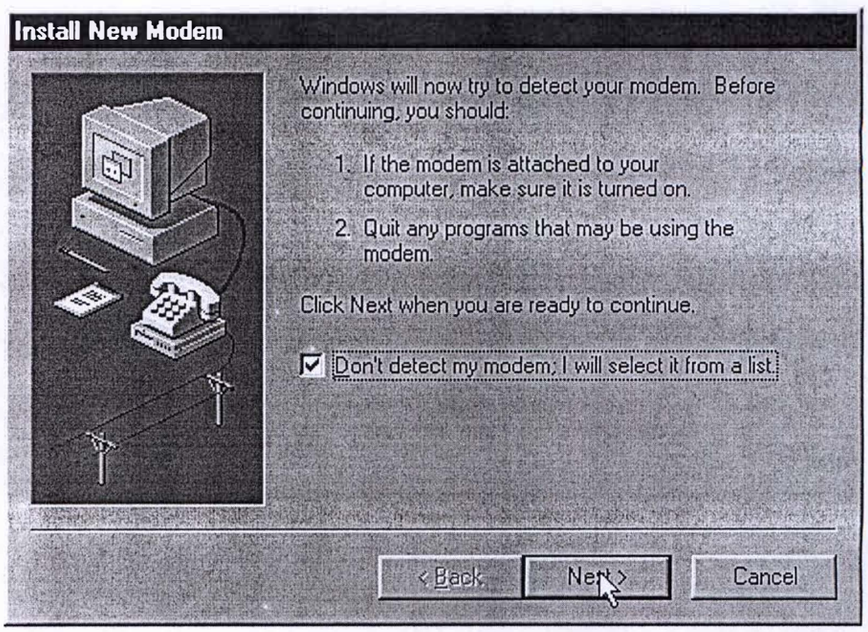
Jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta terhubung dengan *backbone* internet melalui *Internet Service Provider* (ISP) di Yogyakarta sehingg dapat dimanfaatkan untuk akses internet. Untuk akses internet diperlukan *setting* koneksi. Adapun *setting* akses Internet/Extranet melalui saluran telepon adalah sebagai berikut :

a. *Install Modem*

Modem merupakan perangkat perantara antara komputer dengan saluran telepon agar dapat berhubungan dengan *ISP* (*Internet Service Provider* - penyedia jasa internet).

1) Klik ***Start***, pilih ***Settings***, pilih ***Control Panel***, akan muncul *window* ***Control Panel***.

2) Pada windows ***Control Panel***, pilih *icon* ***Modem*** dan klik dua kali sehingga muncul *window* ***Instal New Modem*** (bagi yang pernah memasang *modem* sebelumnya akan tampil *window* ***Modem Properties.*** Bila ingin menambah *driver modem* baru, klik ***Add***).

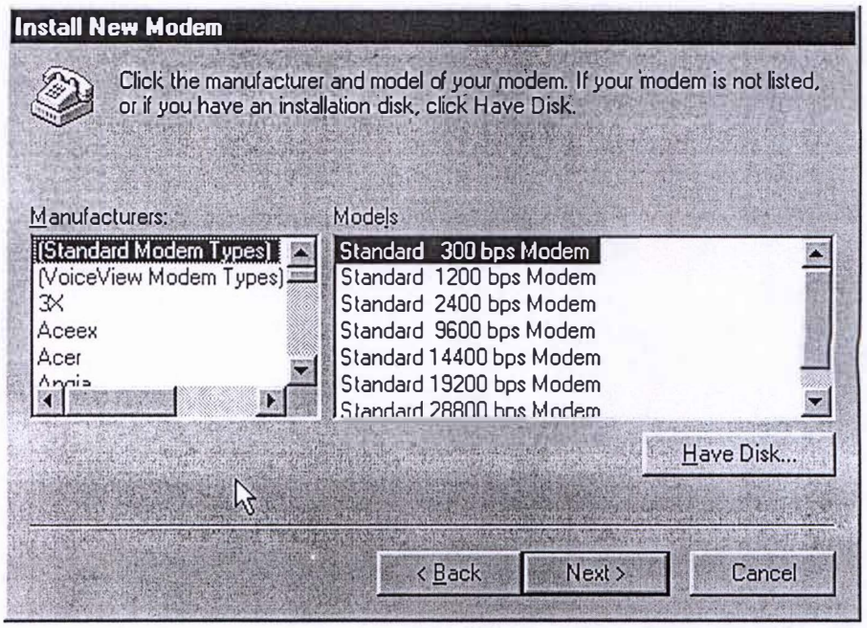


Windows dapat melakukan deteksi otomatis terhadap perangkat *modem* yang telah terpasang pada *PC*, tapi terbatas pada *modem* yang telah dikenali oleh Windows. Apabila memilih deteksi otomatis, maka kosongkan kotak ***Don't detect my modem***, lalu tekan ***Next.***

Apabila dengan *modem* jenis baru dan disertai *file driver* (dalam disket / CDROM), sebaiknya memilih deteksi manual sehingga dapat memanfaatkan fitur terbaru dari *modem* tersebut (misalnya kemampuan *support* 56 kbps, *fax*, *voice*). Untuk itu pilih kotak ***Don't detect my modem***, dan tekan ***Next.***

3) Pada menu selanjutnya ditampilkan daftar *modem* yang telah dikenali dan tersedia *driver*-nya oleh Windows. Pilih ***type modem*** yang sesuai lalu tekan ***Next***.

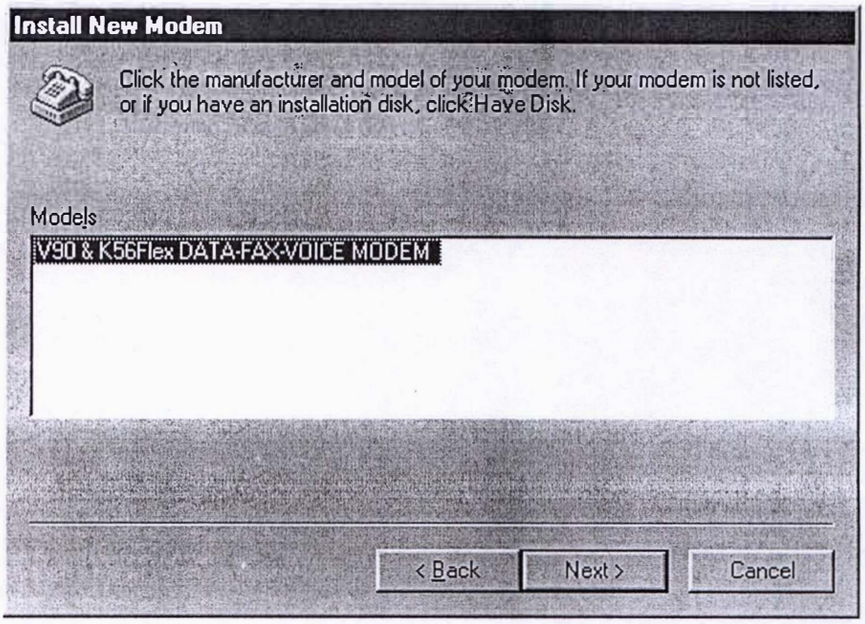
Apabila tidak memiliki *file driver*, dapat memilih ***type Standard Modem***, misalnya dengan kecepatan 28800 bps, lalu tekan ***Next*** selanjutnya dapat langsung menuju ke langkah 5.



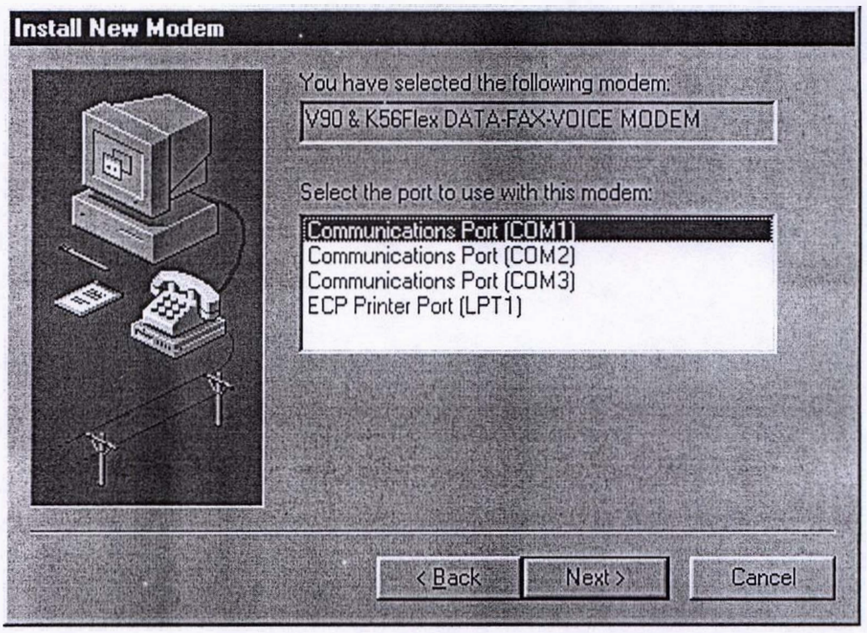
Apabila memiliki *file driver* (disket / CDROM) yang disediakan pabrikan, maka pasang disket / *CDROM* tersebut, lalu tekan tombol ***Have Disk***.

4) Pada menu selanjutnya muncul *window* ***Install From Disk***. Masukkan disket / *CDROM* yang berisi *file driver modem*, pilih *drive* yang sesuai (A:\ atau pilih ***CDROM***, lokasi lain menggunakan menu ***Browse***).

5) Apabila *file driver* berhasil di ambil, maka akan muncul *window* mengenai *driver* tersebut (pada contoh ini, *driver modem* V90 & K56Flex *DATA-FAX-VOICE Modem*, yang memiliki kemampuan s/d 56 kbps). Pilih *driver* yang sesuai (bila lebih dari satu), selanjutnya tekan ***Next***.



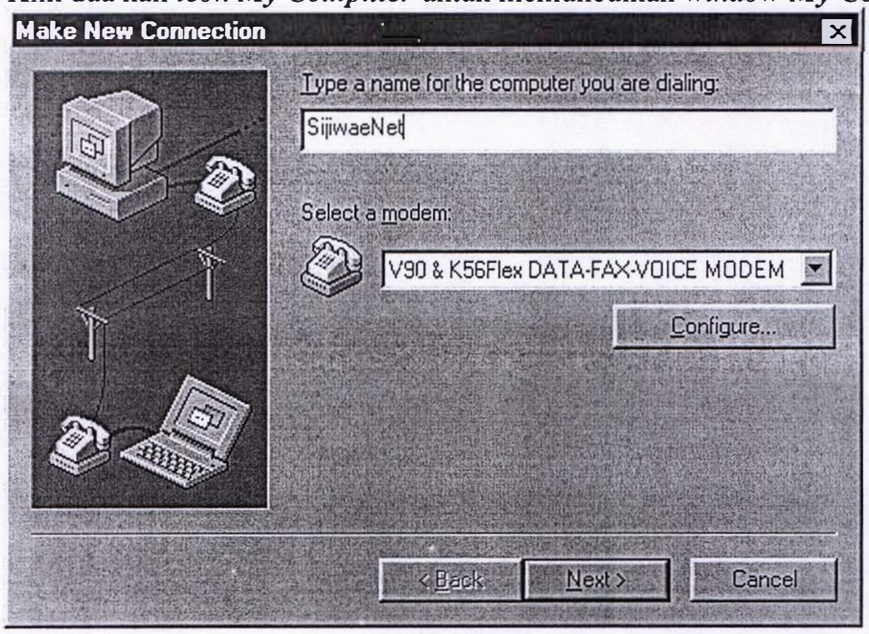
6) Setelah selesai, harus menentukan *port* komunikasi (*COM*) dimana *modem* tersebut terpasang. Sebagai contoh, dipilih *port COM1* karena biasanya *modem* terpasang pada *port* tersebut (kecuali dipakai untuk media lain). Kemudian tekan *modem*.



Bila tahap ini dilakukan dengan benar, maka *modem* akan terpasang pada *PC*. Klik ***Finish*** untuk mengakhiri *setup modem*.

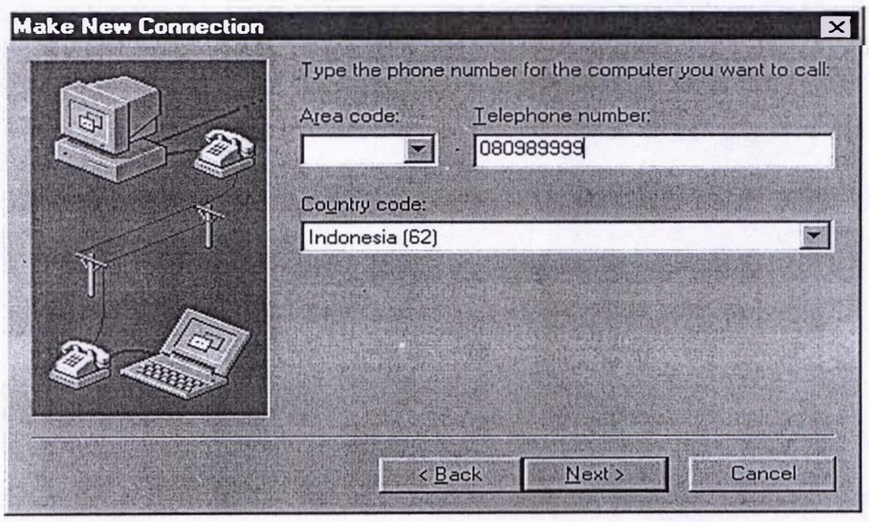
b. *Setting Dial-up*

1) Klik dua kali *icon* ***My Computer*** untuk memunculkan *window* ***My Computer.***



2) Klik dua kali *icon* ***Dial Up Networking.*** Setelah muncul *window* ***Dial up Networking,*** klik dua kali *icon* ***Make New Connection.*** Pada *window Make New Connection*, masukkan nama ***SijiwaeNet*** pada kolom pertama untuk nama komputer yang akan di-dial dan pilih jenis *modem* yang telah diinstalasi. Tekan ***Next.***

SijiwaeNet menggunakan nomor akses khusus yang tidak memerlukan kode area, karena itu kosongkan pada kolom ***area code.*** Ketik nomor telepon akses ***SijiwaeNet*** pada kolom nomor telepon, yaitu **0 809 8 9999,** klik ***Next.***

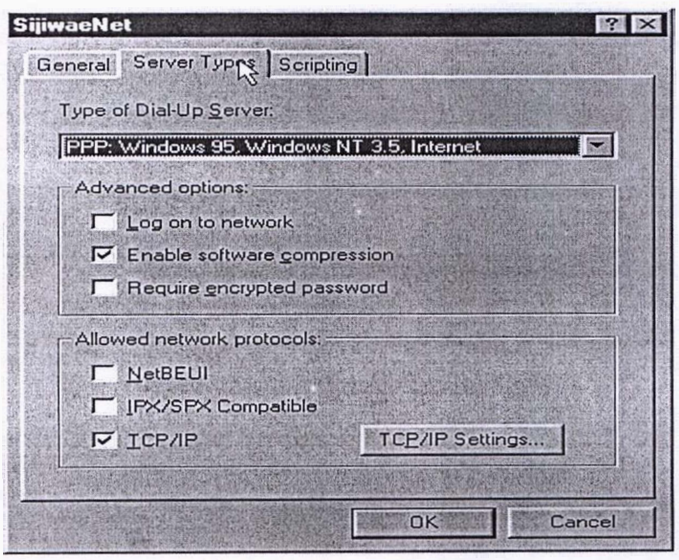


3) *Setting* koneksi selesai, klik ***Finish***. Pada tahap ini telah berhasil melakukan *setting dial up* yang ditandai dengan keluarnya *icon SijiwaeNe*t pada *window* ***Dial Up Networking.***
Setelah selesai tahap ini, dapat melakukan ***setting*** **DNS.**

c. *Setting DNS* (*Domain Name Server*)

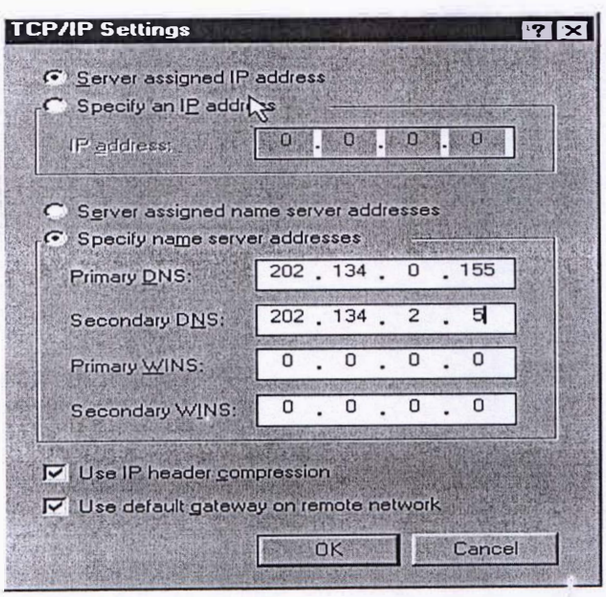
Fungsi dari *setting* DNS adalah untuk menentukan alamat *IP server* yang berfungsi sebagai ***Domain Name Server*** (*server* ini bertugas menerjemahkan alamat domain yang dituju). *Setting* ini sebaiknya dilakukan, walaupun bukan merupakan kerharusan karena *SijiwaeNet* akan secara otomatis menentukan *DNS server*.

1) Klik dua kali *icon* ***My Computer***, lalu klik dua kali *icon* ***Dial Up Networking.***
2) Klik kanan *icon SijiwaeNet* yang sudah dibuat sebelumnya, pilih ***Properties***.
3) Setelah keluar *window* ***SijiwaeNet***, klik pada ***Server Types*** *Tab*. Perhatikan *setting* pada ***Advanced Options***, lakukan seperti terlihat pada gambar.



4) Klik tombol ***TCP/IP Settings***. Klik pada ***Specify name server address***, lalu isikan sebagai berikut :

Masukkan *Primary DNS* : **202.134.0.155** dan *Secondary DNS* : **202.134.2.5**



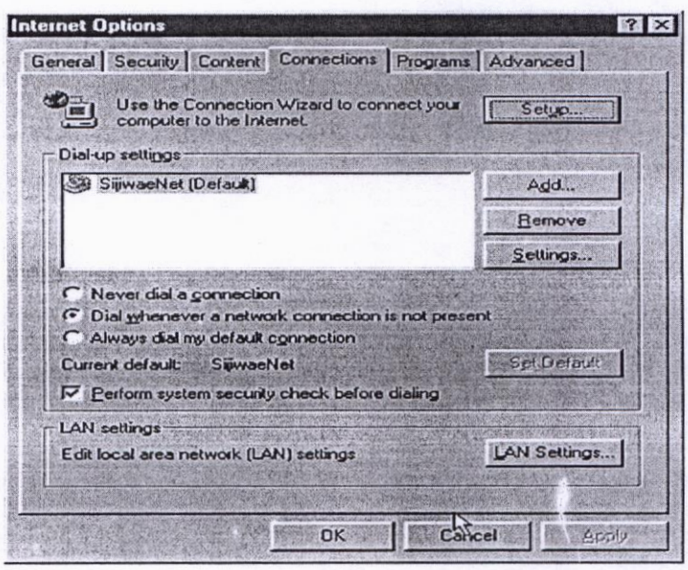
Setelah selesai, klik ***OK*** untuk menutup dialog, lalu ***OK*** lagi untuk kembali ke awal.

d. *Setting Proxy Server*

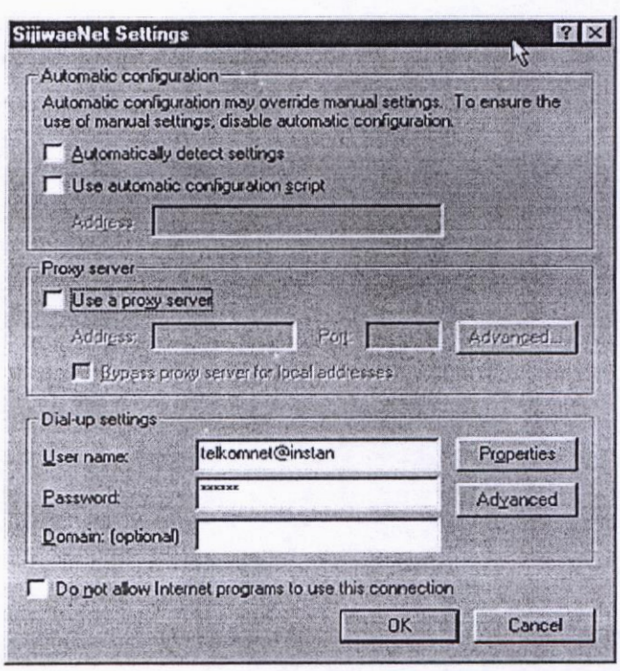
Proxy server adalah *server* untuk menyimpan halaman *web* yang pernah diakses oleh pengguna, untuk mempercepat akses situs *web* . Dengan *proxy server*, pengakses yang akan melihat halaman *web* tidak perlu harus selalu mengakses secara langsung ke *server* penyimpan sebenarnya, tetapi cukup melihat pada *cache proxy server* setempat.

Seting proxy server dapat dilakukan melalui aplikasi *browser* (baik ***Internet Explorer / IE*** maupun ***Netscape Navigator***). Untuk IE versi 5.O, adalah sebagai berikut :

1) Jalankan ***Internet Explorer***, klik menu ***Tools***, lalu pilih ***Internet Options***. Maka akan muncul *window* ***Internet Options***, pilih *tab* ***Connection*** sehingga muncul seperti dibawah.



2) Pada kotak ***Dial-up settings***, misalnya pilih **SijiwaeNet** (pilihan ini seharusnya muncul bila telah membuat *setting dial up modem* sebelumnya). Kemudian tekan tombol ***Settings***. Maka akan muncul *window SijiwaeNet Settings* seperti di bawah.

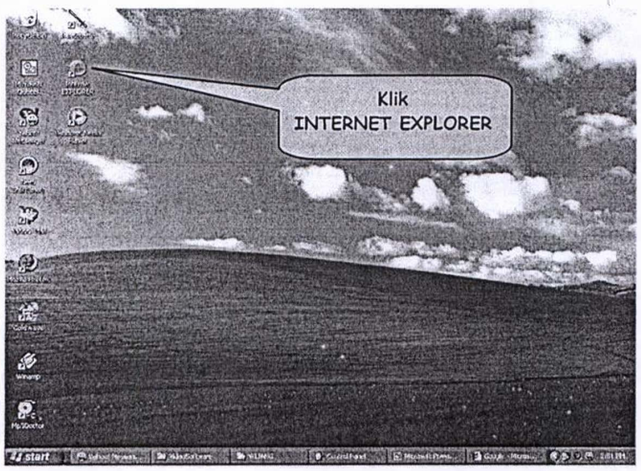


3) Perhatikan pada kotak ***Proxy Server***. Pada ***Use a proxy server***, kotak pilihan **dikosongkan** (tidak diberi tanda). Artinya, memberikan seting agar *browser* tidak usah menggunakan *proxy*. Hal ini dilakukan karena untuk akses lewat SijiwaeNet, seluruh pengguna telah diset agar secara otomatis agar menggunakan *proxy* Telkom secara *default*, sehingga tidak perlu dilakukan seting.

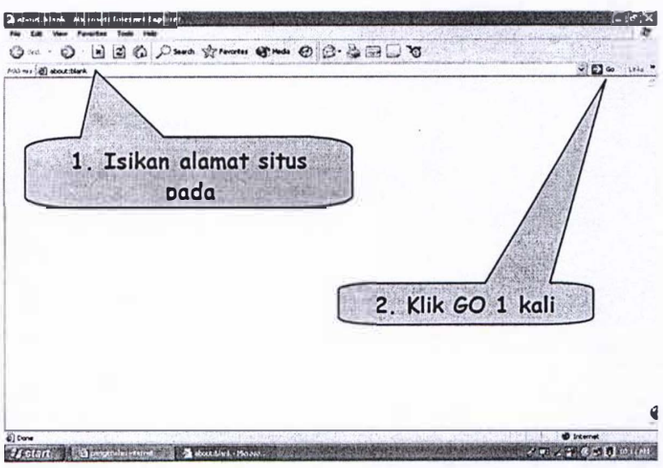
4) Klik tombol **OK**. Maka *seting proxy* telah selesai.

e. Cara Mengakses Internet :

1) Untuk mengakses Internet diperlukan *software browser*, seperti *Internet Explorer, Firefox, Opera*, dan lain-lain.
2) Untuk pencarian informasi melalui internet dapat menggunakan mesin-mesin pencari (*Search Engine*) seperti : *Google.com, Yahoo.com*, *Altavista.com*, dan lain-lain.
3) Dalam akses internet perlu kehati-hatian atas adanya virus ketika *download* file-file yang berekstensi " *exe*".
4) Adapun cara mengakses internet menggunakan *Internet Explorer* adalah sebagai berikut :
   a. Aktifkan *Internet Explorer* yang terlihat dalam tampilan *desktop* dengan mengklik 2 kali.



   b. Setelah *Internet Explorer* aktif : Dapat membuka berbagai situs internet dengan mengisikan alamat *URL* (*Uniform Resource Locator*)-nya pada ***address bar*** dalam *Internet Explorer*.



f. Meningkatkan Fungsi *Pop-up Blocker* pada *Internet Explorer*

Pop-up adalah gangguan yang muncul dalam penggunaan *Internet Explorer*, berupa jendela-jendela baru yang berisi iklan produk atau bahkan situs porno, kadang situs tersebut terus menerus membuka dirinya sehingga menyebabkan *PC* menjadi *hang* karena kehabisan memori. Untuk menghindari masalah tersebut, pada umumnya ditempuh :

1) Beralih ke *browser* alternatif seperti *Opera* atau *Firefox* yang tidak "bermasalah" dengan *pop-up*.
2) Meng-*install add on* untuk *Internet Explorer* yang telah dirancang khusus menangani *pop-up*.

Langkah itu tetap memerlukan tempat tambahan di *harddisk* untuk menyimpan program. Untuk mengatasi hal itu, Microsoft mengintegrasikan fungsi *Pop-up Blocker* pada *Service Pack 2*-nya untuk Windows XP. Jika telah di-*install* Windows XP SP2, otomatis akan mendapatkan fitur *Pop-up Blocker* ini dengan *setting medium*; pemblokiran *pop-up* dilakukan jika *Internet Explorer* mendeteksi adanya *script* yang secara otomatis meminta membuka jendela baru.

Pada *setting* ini tidak ada jaminan bahwa *pop-up* seratus persen akan terblokir, untuk mengatasinya gunakan trik berikut:

1) Klik ***Start > Control Panel > Network and Internet Connections > Internet Options.***
2) Pilih *tab* **Privacy** pada jendela Internet Properties yang muncul.
3) Pastikan *check box* ***Block Popups*** pada *Pop-up* Blocker sudah diberi tanda.
4) Tekan tombol ***Settings...*** yang terdapat di bagian kanan *check box* ***Block Pop-ups.***
5) Pada bagian ***Filter level***, ubahlah menu *drop down* yang sebelumnya berada pada posisi ***Medium: Block most automatic pop-ups*** menjadi ***High: Block all pop-ups (Ctrl to override).***
6) Tutup jendela ***Pop-up Blocker Settings*** dengan mengklik tombol ***Close*** kemudian klik ***OK***.

Trik ini hanya dapat digunakan jika telah diinstal *Service Pack 2* untuk Windows XP. Jika belum memilikinya dapat *download* secara gratis melalui situs Microsoft.

2. *Email*

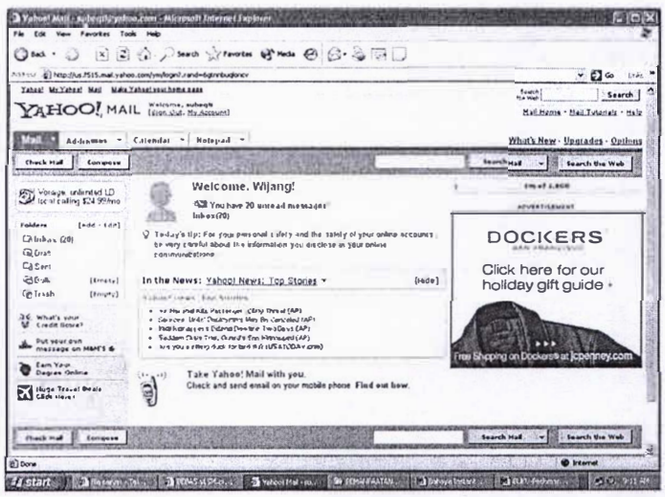
Jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta yang terhubung degan *backbone internet* dapat dimanfaatkan untuk komunikasi dengan *email* melalui internet. Alamat *Email* dapat dibuat melalui penyedia *mail server* untuk umum secara gratis seperti : ***www.mail.yahoo.com; www.Hotmail.com; www.mailcity.com; www.kompas.com; www.astaga.com.*** Alamat *email* juga dibuat dengan menyediakan *mail server* tersendiri di Badan Informasi Daerah Propinsi Daerah Istimewa Yogyakarta.

Sebagaincontoh **untuk *Mail Yahoo!* caranya adalah sebagai berikut :**

a. Mendaftar *ID* di ***Yahoo!*** dengan :
   1) Aktifkan ***Internet Explorer***;
   2) Ketik alamat pada *address bar* : ***http://mail.yahoo.com***;
   3) Klik ***Sign Up Now***;
   4) Klik ***Sign up for Yahoo! Mail new***;
   5) Isikan pada formulir yang muncul, dan klik ***Submit this form***;
   6) *ID* yang telah dibuat dapat digunakan untuk *Email* di ***Yahoo! Mail*** dan **Yahoo! *Messenger.***

b. Membuka *Email* :

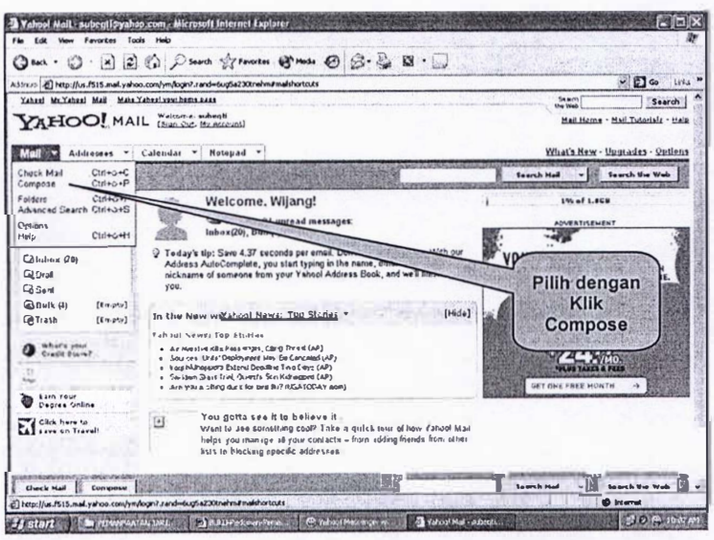
1) Aktifkan ***Internet Explorer.***
2) Ketik alamat pada *address bar* : ***http://mail.yahoo.com.***
3) Setelah muncul halaman baru, isikan data pada ***Yahoo! ID*** *dan* ***Password*** yang telah didaftarkan pada ***Yahoo! Mail.***
4) Klik ***Sign in.***
5) Setelah masuk *Yahoo! Mail* berupa tampilan berikut :



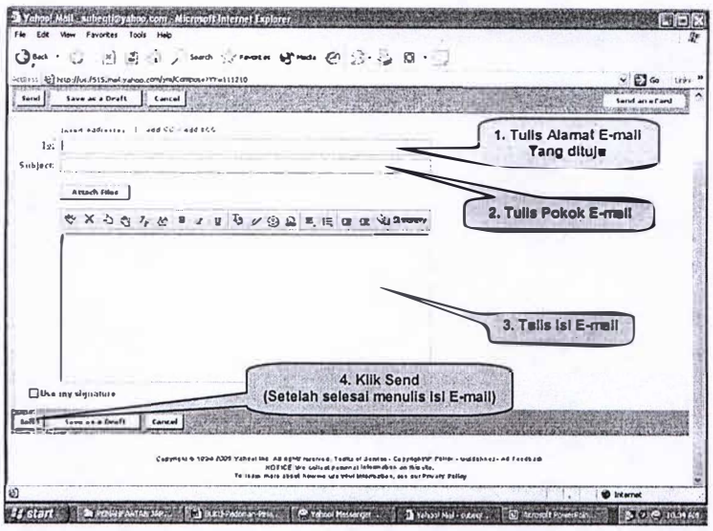
6) Untuk melihat *email* yang masuk klik ***Check Mail*** atau ***Inbox*** (di bagian kiri atas).
7) Setelah keluar halaman yang memuat Daftar *email* yang masuk, untuk membuka *email* klik salah satu *email* yang masuk.

c. Mengirim Email :

1) Setelah *login*, dan masuk halaman berikut.



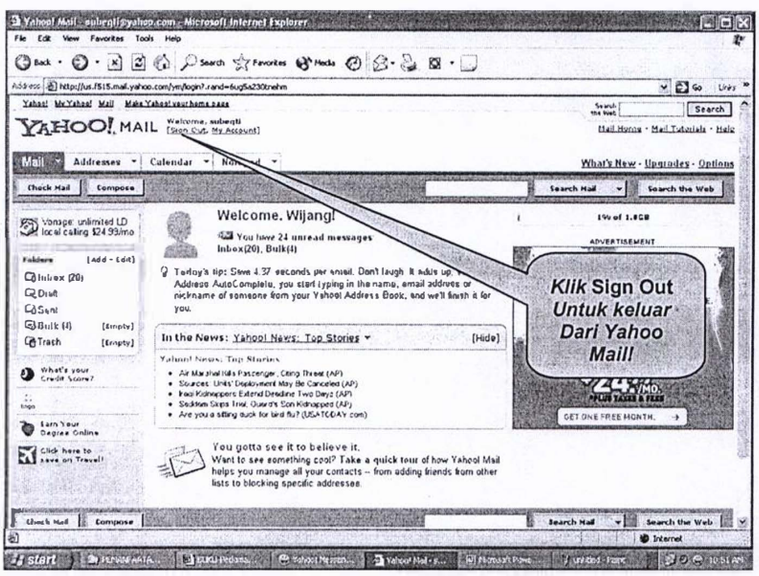
2) Pilih ***Compose.***



3) Tulis Alamat *email* yang dituju.
4) Tulis Subyek *email*.
5) Tulis isi *email*.
6) Setelah selesai klik ***Send*** (pada bagian kiri bawah halaman).

d. Keluar *Email* :

Untuk keluar dari *Yahoo! Mail*, klik ***Sign Out*** (dibagian kiri atas halaman).



3. *Chat*

Jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta yang terhubung degan *backbone internet* dapat dimanfaatkan untuk komunikasi *chat* melalui internet. Komunikasi *chat* dapat dilakukan menggunakan *software Yahoo Messenger.* yang tersedia di internet dan dapat dipergunakan secara gratis untuk di-*download* dan di-*install* dalam komputer. Dengan *chat* komunikasi dapat dilakukan menggunakan teks, suara, maupun gambar. Selain itu melalui *chat* dapat untuk mengirim dokumen elektronik dalam bentuk file.

Chat dengan menggunakan *Instant Messaging* ada efek samping yang tidak dikehendaki. Cara menghindari munculnya masalah dalam penggunaan aplikasi *Instant Messaging* antara lain adalah :

- Sebisa mungkin, jangan menggunakan nama yang bisa menjelaskan identitas pribadi.
- Kecuali sudah menyadari resikonya, jangan memajang *ID* di tempat-tempat umum.

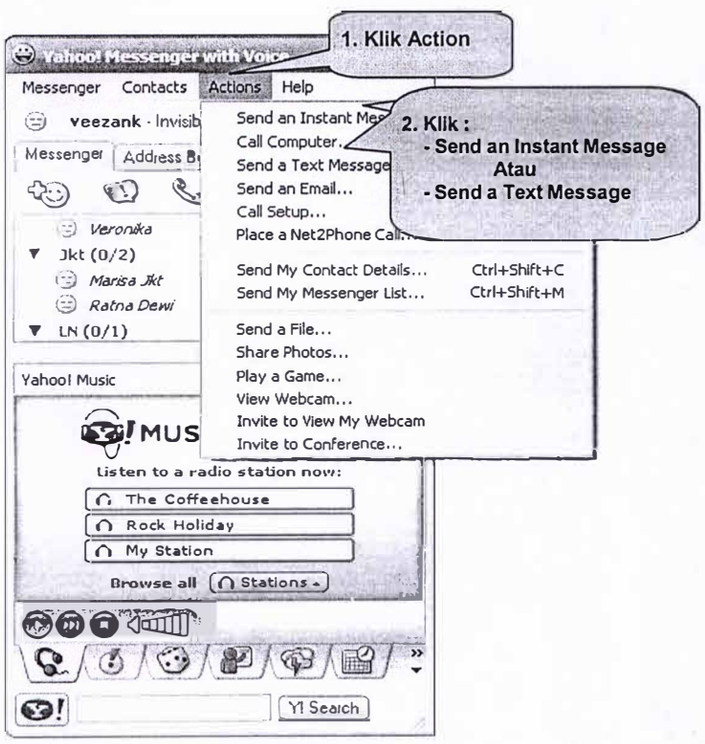
- Pada komputer yang digunakan bersama, setelah selesai menggunakan keluar dari *software Instant Messenger* dan jangan membiarkan *software* tersebut mengingat *ID* dan *password*.
- Sebisa mungkin, menghindari berbicara dengan orang yang tidak ada di daftar kontak (teman).
- Ketika bercakap-cakap menggunakan *Instant Messenger*, jangan menuliskan informasi pribadi seperti nomor kartu kredit atau *password*.
- Menghindari menerima kiriman file dari orang yang belum benar-benar dikenal. Kalaupun sudah kenal dengan orang tersebut, perlu memeriksa apakah file tersebut tidak berbahaya (mengandung virus, *trojan*, dan sebagainya) sebelum membuka atau meng-*install*.
- Menghindari pertemuan langsung dengan orang yang belum benar-benar dikenal walaupun sering bercakap-cakap secara *online* lewat *software Instant Messenger*.

Untuk *Yahoo! Messenger*, Caranya adalah sebagai berikut :

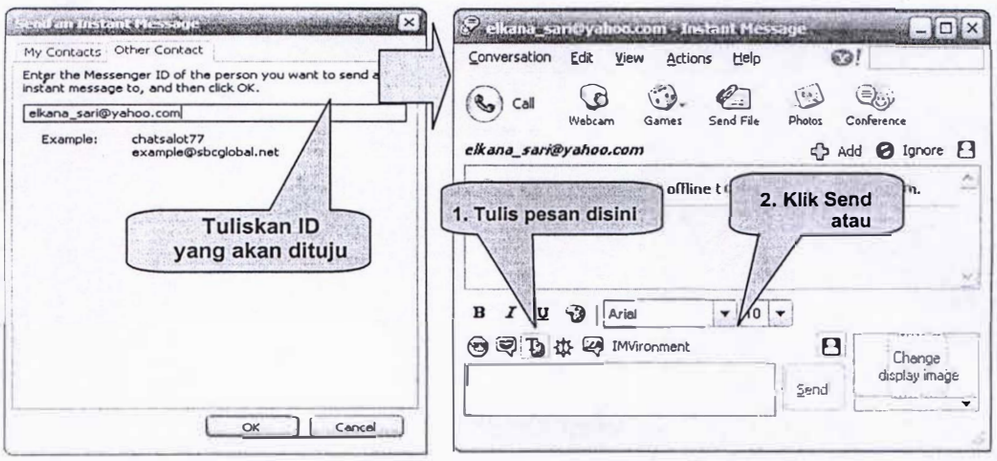
Langkah awal adalah : ***Download*** dan ***install Yahoo Messenger***

a. Mengirim Pesan Teks :

1) Mendaftarkan *ID* di *Yahoo!* Seperti pada *Yahoo! Mail* di atas.
2) Aktifkan *Yahoo!Messenger*.



3) Setelah melakukan sesuai petunjuk gambar diatas, akan muncul halaman baru dan tuliskan *ID* yang dituju.

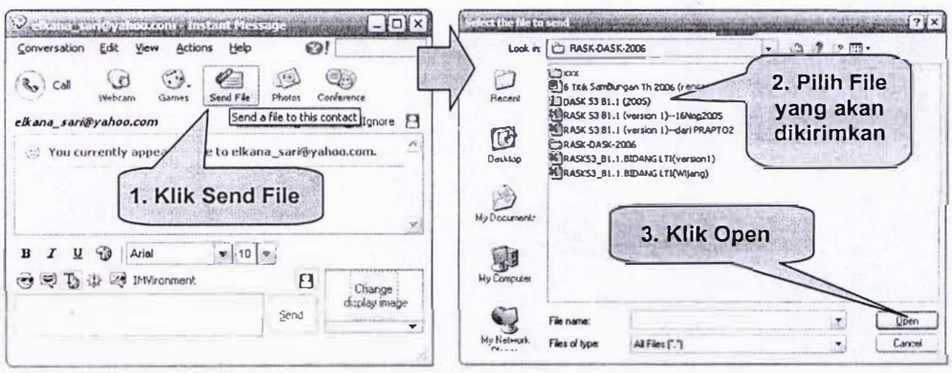


4) Setelah kegiatan 1 dan 2 pada gambar di atas dilakukan maka pesan akan sampai pada *ID* yang dituju.

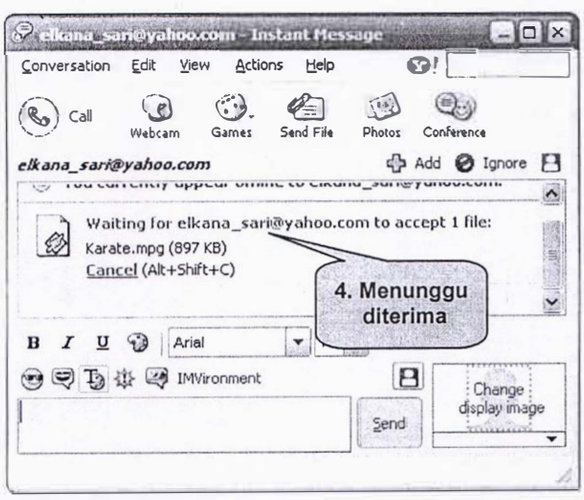
b. Mengirim File :

1) Sebagaimana dalam gambar dibawah, dari jendela *ID* tujuan yang telah terbuka, klik ***Send File*** (angka 1 gambar berikut).

2) Akan muncul jendela baru untuk memilih file yang akan dikirim, Pilih ***File*** (angka 2 gambar berikut).



3) Setelah file dipilih, klik ***Open*** (angka 3 gambar diatas), maka file telah terkirim tinggal menunggu diterima oleh *ID* tujuan (angka 4 gambar berikut).



VI. KEAMANAN JARINGAN

Untuk menjaga kinerja, pemanfaatan jaringan komputer perlu waspada terhadap serangan virus komputer. Serangan virus dapat melumpuhkan sistem komputer baik secara *stand alone* maupun jaringan. Selain virus juga ada ancaman *Cracker*. Jaringan komputer tidak bisa lepas dari kedua hal tersebut, untuk itu sangat diperlukan upaya untuk menjaga keamanan jaringan.

Keamanan jaringan adalah perlindungan terhadap sumber daya jaringan dari upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh seseorang yang tidak diijinkan. Protokol suatu jaringan dapat dibuat aman. Sebuah protokol atau layanan (*service*) dianggap cukup aman apabila mempunyai kekebalan ***Internet Threat Level (ITL)*** klas 0.

A. *Threat* (Ancaman)

Keamanan jaringan terkait dengan adanya ancaman ***(threat)*** dari pengguna yang tidah sah. Terdapat dua kategori ***threat*** yaitu **pasif** dan **aktif**.

Threat **pasif** melakukan pemantauan dan atau perekaman data selama data ditransmisikan lewat fasilitas komunikasi. Tujuan penyerang adalah untuk mendapatkan informasi yang sedang dikirimkan. Kategori ini memiliki dua tipe *yaitu release of message contain* yang memungkinan penyusup untuk mendengar pesan dan *traffic analysis* yang memungkinan penyusup membaca *header* suatu paket sehingga bisa menentukan arah atau alamat tujuan paket dikirimkan.

Threat **aktif** merupakan pengguna gelap suatu peralatan terhubung fasilitas komunikasi untuk mengubah transmisi data atau mengubah isyarat kendali atau memunculkan data atau isyarat kendali palsu. Untuk kategori ini terdapat tida tipe yaitu :

- Tipe *message-stream modification* memungkinan pelaku memilih untuk menghapus, memodifikasi, menunda, melakukan *reorder* dan menduplikasi pesan asli. Pelaku juga mungkin untuk menambahkan pesan-pesan palsu.
- Tipe *denial of message service* memungkinkan pelaku untuk merusak atau menunda sebagian besar atau seluruh pesan.
- Tipe *masquerade* memungkinkan pelaku untuk menyamar sebagi *host* atau *switch* asli dan berkomunikasi dengan yang *host* yang lain atau *switch* untuk mendapatkan data atau pelayanan.

1. *Internet Threat Level*

Tingkat keamanan sistem internet diukur dalam skala *Internet Threat Level* (*ITL*). Ancaman terendah digolongkan dalam *ITL* kelas 0, sedangkan ancaman tertinggi digolongkan dalam *ITL* kelas 9. Tabel berikut menjelaskan masing-masing kelas *ITL*.

Kelas	Penjelasan
0	*Denial of service attack* – pengguna tidak dapat mengakses file atau program
1	Pengguna lokal dapat membaca file-file pada sistem lokal.
2	Pengguna lokal dapat menulis dan atau mengaktifkan file-file selain milik *root* pada sistem.
3	Pengguna lokal dapat menulis dan atau mengaktifkan file-file milik *root* pada sistem.
4	Pengguna jarak jauh (*remote users*) dalam jaringan dapat membaca file-file pada sistem atau yang di *transfer* melalui jaringan.
5	Pengguna jarak jauh (*remote users*) dalam jaringan dapat menulis dan atau

	mengaktifkan file-file selain milik *root* pada sistem atau yang di *transfer* melalui jaringan.
6	Pengguna jarak jauh (*remote users*) dalam jaringan dapat menulis dan atau mengaktifkan file-file milik *root* pada sistem atau yang di *transfer* melalui jaringan.
7	Pengguna jarak jauh (*remote users*) dari luar *firewall* dapat membaca file-file pada sistem atau yang di *transfer* melalui jaringan.
8	Pengguna jarak jauh (*remote users*) dari luar *firewall* dapat menulis dan atau mengaktifkan file-file selain milik *root* pada sistem atau yang di *transfer* melalui jaringan.
9	Pengguna jarak jauh (*remote users*) dari luar *firewall* dapat menulis dan atau mengaktifkan file-file selain milik *root* pada sistem atau yang di *transfer* melalui jaringan.

Berdasar kerumitan perilaku ancaman, permasalahan keamanan dapat diklasifikasikan ke dalam 3 kategori utama, yaitu : ancaman bersifat lokal, ancaman bersifat *remote*, ancaman dari lintas *firewall*. Secara lebih rinci klasifikasi itu dapat dipisahkan menjadi : *Read access , Non-root write and execution access, Root write and execution access*.

Tingkat ancaman dapat diukur berdasar beberapa faktor, antara lain : kegunaan sistem, kerahasiaan data dalam sistem, tingkat kepetingan dari integritas data, kepentingan untuk menjaga akses yang tidak boleh terputus, profil pengguna, hubungan antara sistem dengan sistem yang lain.

2. Kriptografi

Untuk keamanan pesan yang dilewatkan jaringan harus menggunakan teknik Kriptografi. Adapun tujuan dari sistem kriptografi adalah :

- *Confidentiality* : memberikan kerahasiaan pesan dan menyimpan data dengan menyembuyikan informasi lewat teknik-teknik enkripsi.
- *Message Integrity* : memberikan jaminan bahwa pesan tidak akan mengalami perubahan dari saat dibuat sampai saat dibuka.
- *Non-repudiation* : memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.
- *Authentication* : Memberikan dua layanan. *Pertama* mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. *Kedua* untuk menguji identitas seseorang apabila ia memasuki sebuah sistem.

Cara untuk membuat pesan tidak mudah terbaca adalah *enkripsi*. Dalam hal ini terdapat tiga kategori *enkripsi* antara lain :

- Kunci *enkripsi* rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk meng-*enkripsi* dan juga sekaligus men-*dekripsi* informasi.
- Kunci *enksripsi public*, dalam hal ini dua kunci digunakan, satu untuk proses *enkripsi* dan yang lain untuk proses *dekripsi*.
- Fungsi *one-way*, di mana informasi di-*enkripsi* untuk menciptakan "*signature*" dari informasi asli yang bisa digunakan untuk keperluan *autentifikasi*.

Enkripsi dibentuk dengan berdasarkan suatu *algoritma* yang akan mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tak bisa dilihat. *Dekripsi* adalah proses dengan *algoritma* yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya. *Algoritma* yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati yang harus secara efektif menghasilkan sebuah bentuk ter-*enkripsi* yang tidak bisa dikembalikan oleh seseorang sekalipun mereka memiliki *algoritma* yang sama.

B. Virus Komputer

Virus komputer adalah serangkaian program komputer yang dapat menyebar dengan cepat melalui jaringan *PC* yang terbuka seperti internet. Virus komputer memiliki kemampuan menulari, manipulasi, mengubah bahkan merusak program-program di dalam kompuer yang telah terinfeksi. Akibatnya, virus yang telah dimodifikasi berpotensi menimbulkan banyak gangguan dari mulai merusak atau menghapus sistem file sampai mengganggu sistem operasi *PC*, sehingga tidak mampu bekerja secara normal.

Dari banyak jenis virus yang beredar saat ini secara umum dapat dikelompokkan dalam dua kategori

1. Jenis-Jenis Virus berdasar cara penyebaran :

Berdasar cara penyebarannya, jenis virus dikelompokkan menjadi dua kategori :

a. ***Virus Worm*** **:**

Suatu program yang didesain menyerupai virus dan mampu menggandakan diri sendiri dari satu *PC* ke *PC* yang lain, ***worm*** mampu mengambil alih kontrol pada fitur-fitur di dalam *PC* dengan cara bergerak dalam file atau informasi. Sekali terdapat ***worm*** di di dalam komputer, dia akan menjelajah sendiri. Bahaya terbesarnya adalah kemampuannya untuk menggandakan diri dalam volume yang besar. Sebagai contoh ***worm*** dapat mengirimkan *copy* dari diri sendiri kepada masing-masing orang yang terdapat dalam *email address book*, dan *PC* yang telah tertular akan melakukan hal yang sama. Hal itu berakibat beratnya *traffic network* yang sehingga kinerja jaringan komputer menurun secara keseluruhan.

b. ***Virus Trojan*** **:**

Sesuatu yang kelihatan seperti *software* biasa tetapi program tersebut dapat melumpuhkan *security* dalam suatu program yang lain sehingga menyebabkan kerugian bahkan kerusakan besar. Biasanya ***trojan*** disebut pula *Spy Ware*. ***Trojan*** biasanya terdapat di dalam *email* dalam bentuk *attachment* yang mengklaim diri sebagai *security update* tapi berubah menjadi virus yang dapat merusak program. ***Trojan*** menyebar pada saat membuka suatu program karena biasanya program tersebut berasal dari sumber terpercaya. ***Trojan*** juga terdapat di dalam *software* yang biasa di-*download* secara bebas *(free)*.

2. Jenis virus berdasar serangnannya

Berdasar serangnannya, jenis virus dikelompokkan menjadi enam kategori:

a. ***Virus boot-sector*** **:**

Memasukkan dirinya ke dalam *boot-sector*--sebuah area pada *hard drive* (atau jenis *disk* lainnya) yang akan diakses pertama kali saat *PC* dinyalakan. Virus jenis ini dapat menghalangi *PC* untuk melakukan *booting* dari *hard disk*.

b. ***Virus file*****:**

Menginfeksi aplikasi. Virus ini melakukan eksekusi untuk menyebarkan dirinya pada aplikasi dan dokumen yang terkait dengannya saat file yang terinfeksi dibuka atau dijalankan.

c. ***Virus makro*****:**

Ditulis dengan menggunakan bahasa pemrograman *makro* yang disederhanakan, dan menginfeksi aplikasi *Microsoft Office*, seperti *Word* dan *Excel*. Sebuah dokumen yang terinfeksi oleh *virus makro* secara umum akan memodifikasi

perintah yang telah ada dan banyak digunakan (seperti perintah "*Save*") untuk memicu penyebaran dirinya saat perintah tersebut dijalankan.

d. ***Virus multipartite*:**

Menginfeksi baik file dan *boot-sector*, serta dapat menginfeksikan sistem terus menerus sebelum ditangkap oleh *scanner* antivirus.

e. ***Virus polymorphic*:**

Akan mengubah kode dirinya saat dilewatkan pada mesin yang berbeda; secara teoritis virus jenis ini lebih susah untuk dapat dideteksi oleh *scanner* antivirus, tetapi dalam kenyataannya virus jenis ini tidak ditulis dengan baik, sehingga mudah untuk diketahui keberadaannya.

f. ***Virus stealth*:**

Menyembunyikan dirinya dengan membuat file yang terinfeksi tampak tidak terinfeksi, tetapi virus jenis ini jarang mampu menghadapi *scanner* antivirus terbaru.

3. Jenis-jenis Virus Terkenal dan mempengaruhi jaringan (*LAN* dan *WAN*)

Virus yang juga merupakan *worm* yang dapat mempengaruhi jaringan khususnya jaringan komunikasi. Virus tersebut adalah

a. ***Blaster* :**

Sebuah kode/program kecil yang membuat windows menjadi musuh dari windows yang lain. *Blaster* biasanya menyerang *port* 135 RPC (*remote procedure call*) salah satu komponen pada windows selain menyerang *port* 135 RPC, *Blaster* merupakan virus *worm* yang menyerang *PC user*. Penyebaran *Blaster* melalui pencarian *port* 135 RPC.

Cara Mengatasi :

- Mengfungsikan *Firewall.*
- Meng-*install* "*required update*" dari *security updates* Microsoft yang diluncurkan dengan kode *update* 823980 dan 824146.
- Mengecek dan membuang *Blaster.*

b. **Nachi :**

Secara definisi, *Nachi* sama dengan *Blaster* hanya berbeda cara menyerangnya. *Nachi* menyerang dengan metode *pink test* dengan data kosong, melakukan *broadcast* paket *ICNP*, yang diserang adalah *port RPC*, sama seperti *Blaster, Nachi* juga merupakan virus *worm* yang menyerang *PC user*.

Cara Mengatasi :

- Memfungsikan *Firewall.*
- Menginstal "*required update*" dari *security updates* Microsoft yang diluncurkan dengan kode *update* 823980.
- Mengecek dan membuang *Nachi.*

c. **Sasser :**

Secara definisi, *Sasser* sama dengan *Blaster* dan *Nachi* hanya beda cara menyerangnya dimana *Sasser* menyerang *LSASS* (*Local Security Authority Subsystem Service*) yaitu lisensi windows atau protokol lisensi *window*. Penyebarannya melalui *TCP Port* 445 (*netbios*) yang ada di *PC*, bila ada kelemahan pada *TCP port* 445 akan diserang, sama halnya dengan *Blaster* dan *Nachi, Sasser* juga merupakan virus *worm* yang menyerang *PC user*.

Cara Mengatasi :

- Memfungsikan *Firewall.*
- Menginstal "*required update*" dari Microsoft *Security Bulletin* MS04 – 011.
- Mengecek dan membuang *Sasser.*

d. Mydoom :

Virus yang menyerang ke luar *PC user*/ke arah jaringan dapat juga menyerang ke situs-situs internet, sebagai contoh IBM SCO Unix, dengan cara mengirimi paket WWW. Penyebarannya melalui *email* dan yang diserang adalah *mail server.*

Cara Mengatasi :

- Mengecek dan membuang *Mydoom.*
- Meng-*install* dan memfungsikan *Firewall.*

4. Inveksi virus Komputer

Proses infeksi virus komputer dapat terjadi melalui berbagai cara dan media, oleh karena itu hal-hal berikut perlu diwaspadai yaitu:

a. Menyalin ataupun men-*download* sebuah file yang terinfeksi virus ke dalam *PC* maupun melalui *floppy disk.*

b. Menerima *email* dari internet yang terdapat *attachment* di dalamnya yang terinfeksi virus, karena dengan meningkatnya pemakai internet, maka penyebaran virus adalah melalui *attachment email.*

c. Membuka file/aplikasi, dengan pesan *error,* serta file/aplikasi tersebut tidak jalan dan tidak dapat dibuka.

d. Pada saat hendak dihidupkan, *PC* dengan tiba-tiba men"*shut down*" dengan sendirinya.

e. Men-*download*, meng-*copy*, mengeksekusi file-file yang tidak dikenal.

f. Kinerja jaringan *LAN* ataupun jaringan *WAN* tiba-tiba menjadi lambat sehingga memakan waktu yang cukup lama.

g. Ada beberapa file di dalam *PC* yang hilang dan *hard disk* mendadak menjadi penuh serta kinerjanya menjadi lambat.

5. Petunjuk Umum Pencegahan Virus

Beberapa hal yang perlu dilakukan untuk mencegah berjangkitnya virus di komputer adalah :

a. *Email attachment* jangan dibuka secara otomatis. Jika menggunakan ***Outlook Express, Outlook, Eudora, Netscape,*** dan sebagainya program *email* tersebut perlu disetel agar *attachment* tidak membuka secara otomatis.

b. Hanya buka *email attachment* dari pengirim yang dikenal. Sebelum membuka *attachment*, perlu di-*scan* terlebih dahulu. Hal ini juga berlaku bagi pengguna *web-mail* seperti *yahoo, hotmail*, dan sebagainya.

c. Jangan membuka *email attachment* yang dicurigai mengandung virus walaupun *email* tersebut berasal dari orang yang dikenal. Konfirmasi terlebih dahulu dengan pengirim sebelum membukanya.

d. Jangan membuka *email attachment* dengan ekstensi ***VBS, SHS***, atau ***PIF***. Ekstensi tersebut umumnya digunakan oleh virus dan *worms*.

e. Jangan membuka *email attachment* dengan ekstensi ganda, seperti **nama_file.*BMP.EXE*** atau **nama_file.*TXT.VBS***.

f. Apabila menerima *email* berupa iklan, jangan membuka *attachment*-nya ataupun membuka/mengikuti *web link* yang disertakan.

g. Jangan membuka *email attachment* dengan nama file yang *sensual*. *Email* bervirus sering mengunakan nama file yang menggoda.

h. Jangan mempercayai *icon* yang disertakan dalam *attachment*. *Worm* sering mengirimkan file bervirus dengan *icon* yang mirip dengan *icon* gambar, teks, ataupun file.

i. Menghindari membuka *attachment* dari orang tak dikenal pada saat *chatting* dengan menggunakan *IRC, ICQ* atau *Instant Messenger*.

j. Menghindari men-*download* file dari *newsgroup publik* yang tidak dikenal karena media tersebut sering digunakan oleh pencipta virus untuk mendistribusikan virusnya. Termasuk di dalamnya adalah *freeware* (program gratis), *screensavers*, *game*, dan berbagai program yang bisa dieksekusi (biasanya menggunakan ekstensi ***.EXE*** atau ***.COM***).

k. Apabila harus men-*download* file dari Internet, pastikan melakukan *scanning* terlebih dahulu sebelum membuka program tersebut. Lakukan *Download* semua file dalam satu *folder*, kemudian lakukan *scanning* atas *folder* tersebut.

l. Tidak menjalankan program yang tidak dikenal, terutama file yang bisa di eksekusi yaitu ***.com, bat*** dan ***.exe***

m. Jangan melakukan *share folder* komputer. Apabila harus melakukan *sharing*, jangan keseluruhan *drive* (misal seluruh drive C) atau direktori Windows – dan lindungi *sharing folder* tersebut dengan *password*.

n. Meng-*install* dan selalu meng-*update software scanning anti virus* dan selalu men-*download virus definition update*- nya secara teratur.

o. Konfigurasikan agar program antivirus bekerja setiap kali komputer melakukan *booting* dan bekerja setiap saat (perhatikan *icon V-shield* harus muncul di *tray desktop* komputer).

p. Selalu melakukan *scanning floppy disk* sebelum menggunakannya.

q. Jangan melakukan *booting* dari *floppy disk*, *CD, USB*, atau media sejenis. Untuk menghindari *booting* tidak sengaja dari media tersebut, selalu keluarkan media tersebut dari *disk drive* setiap kali selesai bekerja, dan perlu merubah sistem ***BIOS*** agar komputer tidak melakukan.

r. Hilangkan program a*utorun*. Fasilitas *autorun* biasa dimanfaatkan oleh virus di *CD* yang akan menjalankan dirinya sendiri tanpa diketahaui. Untuk itu disarankan menghilangkan fasilitas *autorun CD,* dengan cara :
   1) ***Control Panel, System.***
   2) ***Device Manager.***
   3) ***CDRom.***
   4) ***Autoinsert Notivication.***

s. Gunakan internet *firewall*.

6. **Tindakan yang perlu dilakukan jika PC terinfeksi Virus :**

   a. Deteksi dan tentukan darimana asal dan lokasi virus tersebut. Misalnya disket, *email* dan sebagainya. Jika virus datang dari disket (*external device*), sebaiknya disket yang terinfeksi tidak lagi digunakan. Jika berasal dari *email* cobalah untuk membuat aturan (*rule*) dengan memblok mail yang memiliki subyek.

   b. Jika *PC* terhubung ke internet, baik melalui jaringan *LAN* maupun dengan akses *dial up*, sedapat mungkin putuskan hubungan tersebut. Hal ini perlu dilakukan agar virus tidak menginfeksi *PC* lain melalui jaringan.

   c. Identifikasi pesan *error* (kesalahan) yang timbul misalnya *file corrupt* atau terhapus. Hasil identifikasi ini bisa digunakan sebagai acuan jika akan mencari ke situs tertentu untuk mendapatkan antivirusnya.

   d. *Scan* dengan antivirus yang telah terpasang. Jika *PC* telah terinfeksi cobalah *update* antivirus, jika virus teryata memblok akses untuk *update*, gunakanlah *PC* lain dan segera *scan hardisk* di *PC* tersebut.

   e. Langkah terakhir, jika tetap tidak bisa dibersihkan, usahakan selamatkan file yang belum terinfeksi dan segera format ulang.

   f. Jalan terbaik untuk melindungi *PC* dari virus adalah jika memiliki koneksi ke internet, jangan membuka *email attachment* dari orang yang tidak dikenal dan hindari men-*download* dari sumber yang tidak jelas. Usahakan untuk tidak mengklik-dobel isi *mailbox*. Bila mendapat kiriman sebuah *attachment file* yang tidak diminta, coba ditanyakan kepada si pengirim tentang isi *attachment* dan cara menggunakan file tersebut sebelum dibuka.

7. **Cara Menanggulangi Masalah Yang Diakibatkan *Spyware***

   Beberapa *software* yang dapat meghilangkan semua *spyware* dari komputer, adalah

   a. *SpyBot Search & Destroy*. Dapat di-*download* dari **http://www.safer-networking.org/**. *Install software* ini dan *update database*-nya dengan menekan tombol ***'search for update'***. Tekan tombol ***'Search for Problems'*** dan hapus program yang ditemukannya. Lakukan ***reboot*** pada komputer.

   b. *Ad-aware* keluaran ***Lava-Soft*** **(http://www.lavasoftusa.com/)** *Download free version*-nya dan *install* di dalam komputer. Seperti sebelumnya, *update* dulu *database*-nya dan jalankan. Hapus semua program yang ditemukannya dan lakukan ***reboot*** pada komputer.

   c. Untuk lebih aman ulang sekali lagi kedua langkah di atas sampai semua *spyware* yang ada di komputer tidak ditemukan. Aktifkan program dan *update database*-nya paling tidak seminggu sekali.

   Spyware **bisa masuk ke dalam** komputer karena *setting security* di komputer yang rendah. Untuk menghindari masalah tersebut, dapat dilakukan beberapa hal berikut

   a. Hati-hati dengan program-program yang di-*install*. Banyak program *download* seperti **Kazaa, Imesh** dan lainnya yang meng-*install software* lain secara otomatis yang dapat membuat komputer lambat dan bahkan dapat mebuat komputer *crash*.

   b. *Update* komputer dengan *patch* yang disediakan Microsoft. Di *Internet Explorer*, buka ***Tools > Windows Update > Product Update*** dan *install* semua *security update* yang ada. Penting untuk meng-*update security fixes* ini secara periodik. *Update* juga ***Java VM*** karena banyak juga program yang menggunakannya.

   c. Di *Internet Explorer*, klik ***Tools > Internet Options > Security > Internet***. Tekan tombol ***'default'*** dan tekan ***'OK'***. Sekarang tekan ***'Custom Level'***. Untuk '***ActiveX***', pilih *'prompt'* untuk ***'Download signed and unsigned ActiveX control'***. Pilih

'disable' untuk ***'Download unsigned ActiveX controls'*** dan ***'Initialize and script ActiveX control'.***

d. Ketika mengakses internet biasa ada konfirmasi untuk *install software* di dalam komputer. Untuk *websites* yang sudah diketahui dan dipercayai dapat memindahkannya ke ***'Trusted Zone'*** di ***Internet option > security.***

Bahaya ActiveX

Ketika ***'browser'*** menjalankan ***ActiveX control*** sama dengan memerintahkan komputer untuk menjalan program (*mengistall software*). Untuk itu dapat menggunakan fitur ***'Immunize'*** di ***SpyBot Search & Destroy*** untuk mencegah *website-website* yang tidak diinginkan meng-*install* program di komputer.

Program sama yang juga dapat di-*install* adalah *SpywareBlaster* dari ***Javacool*** (***http://www.wilderssecurity.net***). Program dari *Javacool* lainnya adalah *SpywareGuard* yang bekerja seperti anti virus tetapi untuk mencegah *spyware*. Ada baiknya meng-*install software* ini sebagai tambahan antivirus di dalam komputer. Ada juga *website* menarik untuk *security test browser* di ***http://www.jasons-toolbox.com.***

C. Firewall

Firewall merupakan suatu cara atau mekanisme perlindungan terhadap *hardware*, *software* ataupun sistem itu sendiri, dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen jaringan pribadi (yang dapat berupa sebuah workstation, *server*, router, atau *local area network-LAN*) dengan jaringan luar yang bukan merupakan ruang lingkupnya. Konfigurasi sederhananya adalah sebagai berikut

PC (jaringan lokal) ←→ *firewall* ←→ *internet* (jaringan lain)

1. Karakteristik sebuah firewall

a. Seluruh hubungan/kegiatan ke luar, harus melewati *firewall* . Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati *firewall* .

b. Hanya kegiatan yang terdaftar/dikenal dapat melewati/ melakukan hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal.

c. *Firewall* itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan, hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

2. Metode kerja sebuah firewall :

a. *Service control* (kendali terhadap layanan), bekerja berdasarkan tipe-tipe layanan yang digunakan di Internet dan diperbolehkan diakses untuk kedalam ataupun keluar *firewall* . Biasanya *firewall* akan mencek nomor *IP Address* dan juga nomor *port* yang di gunakan baik pada protokol *TCP* dan *UDP*, bahkan bisa dilengkapi *software* untuk *proxy* yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya.

b. *Direction Conrol* (kendali terhadap arah), bekerja berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diijinkan melewati *firewall* .

c. *User control* (kendali terhadap pengguna), bekerja berdasarkan hak akses pengguna/*user* untuk menjalankan suatu layanan, artinya ada pengguna yang dapat dan ada yang tidak dapat menjalankan suatu layanan, di karenakan pengguna tersebut tidak di ijinkan untuk melewati *firewall* . Biasanya digunakan untuk membatasi pengguna dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

d. *Behavior Control* (kendali terhadap perlakuan), bekerja berdasarkan banyaknya layanan itu telah digunakan. Misal, *firewall* dapat memfilter *email* untuk menanggulangi/mencegah *spam*.

3. Tipe-Tipe Firewall

a. *Packet Filtering Router*

Paket *filtering* diaplikasikan dengan mengatur semua paket *IP* baik yang menuju, melewati atau akan dituju oleh paket tersebut. Pada tipe ini paket akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan paket ini di konfigurasikan untuk menyaring paket yang akan di *transfer* dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada *header IP* dan *transport header*, termasuk alamat *IP* awal dan alamat *IP* tujuan, protokol *transport* yang di gunakan (*UDP,TCP*), serta nomor *port* yang digunakan.

Kelebihan dari tipe ini adalah mudah diimplementasikan, transparan bagi pemakai, relatif lebih cepat. Adapun kelemahannya cukup rumit dalam menyeting paket yang akan disaring secara tepat, serta lemah dalam hal autentikasi. Adapun serangan yang dapat terjadi pada *firewall* dengan tipe ini adalah :

- *IP address spoofing* : *Intruder* (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan *IP Address* jaringan lokal yang telah diijinkan untuk melalui *firewall*.
- *Source routing attacks* : Tipe ini tidak menganalisa informasi *routing* sumber *IP*, sehingga memungkinkan untuk mem-*bypass firewall*.
- *Tiny fragment attacks* : *Intruder* membagi *IP* kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai *TCP header*. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari *TCP header*. Penyerang berharap hanya bagian (*fragment*) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua paket dengan protokol *TCP* dan memiliki *Offset* = 1 pada *IP fragment* (bagian *IP*).

b. *Application-Level Gateway*

Application-level Gateway yang juga di kenal sebagai *proxy server* berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan *layer* aplikasi, baik itu FTP, HTTP, GOPHER.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal *FTP* untuk mengakses secara *remote*, maka *gateway* akan meminta *user* memasukkan alamat *remote host* yang akan di akses. Saat pengguna mengirimkan *user ID* serta informasi lainnya yang sesuai, maka *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada *remote host*, dan menyalurkan data di antara kedua titik. Apabila data tersebut tidak sesuai maka *firewall* akan menolaknya (tidak meneruskan data tersebut). Pada tipe ini *Firewall* dapat di konfigurasikan hanya untuk mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati.

Kelebihannya adalah relatif lebih aman daripada tipe *packet filtering router* dan lebih mudah untuk memeriksa (*audit*) dan mendata (*log*) semua aliran data yang

masuk pada *level* aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan yang akan berakibat penggandaan sambungan koneksi antara pemakai dan *gateway*, dan *gateway* akan memeriksa dan meneruskan semua arus dari dua arah.

c. ***Circuit-level Gateway***

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri, atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe *application-level gateway*. Tipe ini tidak mengijinkan koneksi *TCP end to end* (langsung).

Cara kerjanya : *Gateway* akan mengatur kedua hubungan *TCP* tersebut, satu antara dirinya (*gateway*) dengan *TCP* pada pengguna lokal (*inner host*) serta satu lagi antara dirinya (*gateway*) dengan *TCP* pengguna luar (*outside host*). Saat dua buah hubungan terlaksana, *gateway* akan menyalurkan *TCP* segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (*internal users*).

4. Konfigurasi *Firewall*

a. *Screened Host FIrewall system (single-homed bastion)*

Pada konfigurasi ini, fungsi *firewall* akan dilakukan oleh *packet filtering router* dan ***bastion host***. *Router* ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket *IP* yang menuju *bastion host* yang di ijinkan. Sedangkan untuk arus data (*traffic*) dari jaringan internal, hanya paket *IP* dari ***bastion host*** yang di ijinkan untuk keluar. Konfigurasi ini mendukung fleksibilitas dalam akses internet secara langsung, sebagai contoh apabila terdapat *web server* pada jaringan ini maka dapat di konfigurasikan agar *web server* dapat diakses langsung dari internet. ***Bastion host*** melakukan fungsi *Authentikasi* dan fungsi sebagai *proxy*. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada *packet-filtering router* atau *application-level gateway* secara terpisah.

b. *Screened Host Firewall system (Dual-homed bastion)*

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya dua jalur yang memisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama, adapun untuk *server-server* yang memerlukan akses langsung maka dapat di letakkan ditempat/*segment* yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah *NIC* (*network interface Card*) pada ***bastion host***.

c. *Screened subnet firewall*

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. Karena pada konfigurasi ini di gunakan 2 (dua) buah *packet filtering router*, satu di antara internet dan ***bastion host***, sedangkan satu lagi di antara ***bastion host*** dan jaringan lokal, konfigurasi ini membentuk *subnet* yang terisolasi.

Adapun kelebihannya adalah

- Terdapat 3 (tiga) lapisan/tingkat pertahanan terhadap penyusup/*intruder*.
- *Router* luar hanya melayani hubungan antara internet dan ***bastion host*** sehingga jaringan lokal menjadi tak terlihat (*invisible*).
- Jaringan lokal tidak dapat mengkonstruksi *routing* langsung ke internet, atau dengan kata lain, internet menjadi *Invinsible* (bukan berarti tidak bisa melakukan koneksi internet).

5. Langkah-Langkah Membangun *Firewall*

a. Mengidenftifikasi bentuk jaringan yang dimiliki
Mengetahui bentuk jaringan yang dimiliki khususnya topologi yang di gunakan serta protokol jaringan, akan memudahkan dalam mendesain sebuah *firewall* .

b. Menentukan *Policy* (kebijakan)
Penentuan kebijakan atau *Policy* harus di lakukan, baik atau buruknya sebuah *firewall* yang di bangun sangat di tentukan oleh *policy*/kebijakan yang di terapkan. Diantaranya:
- Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan dibuat.
- Menentukan individu atau kelompok-kelompok yang akan dikenakan *policy* atau kebijakan tersebut.
- Menentukan layanan-layanan yang di butuhkan oleh tiap-tiap individu atau kelompok yang menggunakan jaringan.
- Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman.
- Menerapkankan semua *policy* atau kebijakan tersebut.

c. Menyiapkan *software* atau *hardware* yang akan digunakan.
Perlu dipersiapkan *operating system* yang mendukung atau *software-software* khusus pendukung *firewall* seperti *ip-chains*, atau *ip-tables* pada linux. Serta konfigurasi *hardware* yang akan mendukung *firewall* tersebut.

d. Melakukan test konfigurasi
Pengujian terhadap *firewall* yang telah selesai dibangun harus dilakukan, terutama untuk mengetahui hasil yang akan didapatkan. Caranya dapat menggunakan *tool-tool* yang biasa dilakukan untuk mengaudit seperti *NMAP*.

VI. PENUTUP

1. Mengingat kemajuan teknologi telematika demikian pesatnya baik perkembangan perangkat keras, perangkat lunak, maupun teknologi jaringan, maka sistem jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta ini akan diupayakan selalu meyesuaikan perkembangan teknologi tersebut.
2. Jaringan komputer Pemerintah Propinsi Daerah Istimewa Yogyakarta dikelola, dikembangkan, dipelihara, dan dioptimalkan pemanfaatannya sesuai dengan ketentuan-ketentuan dalam Peraturan Gubernur ini.

GUBERNUR
DAERAH ISTIMEWA YOGYAKARTA,

HAMENGKU BUWONO X