2015

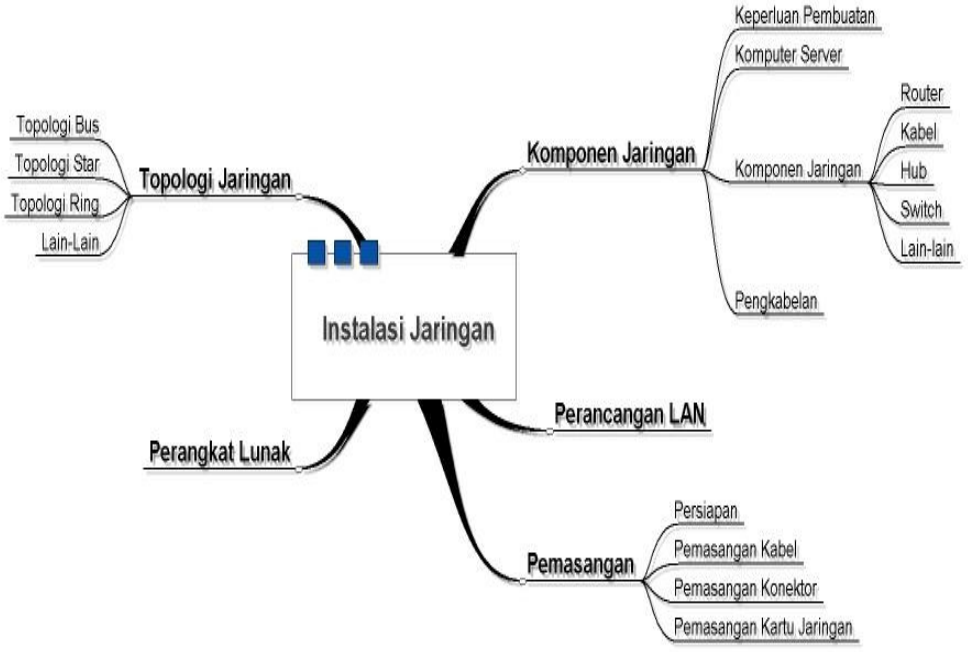
MODUL

JUNIOR NETWORK ADMINISTRATOR

1. TIK.JK01.006.01 Menerapkan Prosedur Kesehatan, Keselamatan dan Keamanan Kerja (K3)
2. TIK.JK02.001.01 Membuat Desain Jaringan Lokal (LAN)
3. TIK.JK02.005.01 Memasang Kabel UTP dan BNC pada Jaringan
4. TIK.JK02.007.01 Memasang Jaringan Nirkabel
5. TIK.JK02.012.01 Menginstal Sumber Daya Berbagi pada Jaringan Lokal
6. TIK.JK02.023.01 Menyelenggarakan Administrasi Sistem Jaringan
7. TIK.JK03.003.01 Mendapatkan Komponen Sistem dari Vendor
8. TIK.JK05.002.01 Melaksanakan Prosedur Perawatan

BAB 1.

Membuat Desain Jaringan Lokal (LAN)



Gambar 1.1. Rincian Pembelajaran

Komponen Jaringan

Agar suatu jaringan LAN atau Workgroup dapat terbentuk, selain harus memiliki komputer Server dan Workstation, juga diperlukan perangkat keras lain yang mendukung jaringan tersebut.

Selain hardware, sistem operasi harus diinstal agar jaringan dapat berfungsi dengan baik. Sistem operasi yang ada antara lain Windows Server 2000, Windows Server 2003, dsb. Untuk lebih jelasnya, akan dijabarkan lebih rinci di bawah ini.

Keperluan Pembuatan Jaringan

Untuk membuat suatu sistem jaringan diperlukan beberapa peralatan antara lain sebagai berikut:

- Sebuah komputer file-server atau yang lebih dikenal dengan **server**, sebagai pusat data.
- Komputer sebagai tempat kerja atau yang disebut dengan **workstation**. Jumlah dari workstation bervariasi, muulai dari satu hingga ratusan.
- NIC (Network Interface Card)
- Wireless LAN
- HUB atau Switch
- Switch Wireless
- Kabel UTP
- Kabel Telepon
- Connector RJ45 dan RJ11
- VDSL Converter
- UPS jika diperlukan

Peralatan jaringan tersebut merupakan kebutuhan standar untuk membuat sebuah jaringan. Apabila jaringan ingin ditingkatkan harus dilakukan penambahan beberapa peralatan sebagai berikut:

- Repeater
- Bridge
- Router
- Gateway

Komputer Server

Server adalah sistem komputer yang berjalan terus menerus di jaringan dengan tugas untuk melayani komputer lain (workstation) dalam jaringan. Banyak server yang memegang peranan tersebut, akan tetapi ada pula yang digunakan secara bersama untuk tujuan lain (misalnya sebagai workstation juga).

Secara fisik, server hampir serupa dengan lomputer pada umumnya, meski konfigurasi hardware lebih sering dioptimisasi untuk memenuhi peranannya sebagai server. Perbedaan antar server dan komputer pada umumnya lebih terletak pada software yang digunakan.

Gambar 1.2. Komputer Server

Server juga secara sering menjadi host dalam mengontrol hardware yang akan di-share pada workstation seperti printer (*print server*) dan sistem file (*file server*). Proses sharing baik untuk kontrol akses dan keamanan, serta dapat mengurangi cost untuk duplikasi hardware (penggunaan hardware dapat optimal).

Beberapa istilah yang berhubungan dengan server adalah sebagai berikut:

- Mail Server

Mail Server memiliki istilah teknis yaitu Mail Transfer Agent (MTA). Mail server adalah suatu aplikasi pada server yang bekerja menerima email datang dari user lokal dan meneruskannya ke user pada domain lain, atau sebaliknya. Penjelasan lebih lanjut dari Mail Server ini akan dijelaskan pada bagian selanjutnya dari modul ini.

- Streaming Media Server

Streaming media adalah media yang digunakan untuk menyebarkan (menyampaikan) sesuatu untuk dikonsumsi (dibaca, dilihat, atau didengarkan). Penyampaiannya menggunakan jaringan. Contoh dari streaming adalah radio dan film (televisi).
Contohnya user dapat meminta video atau suara. Akan tetapi user tidak mempunyai kontrol penuh terhadap dan hanya terjadi komunikasi satu arah, yang dikenal dengan Video on Demand.
Untuk situs yang berisikan aplikasi streaming dibutuhkan suatu server streaming untuk memproses layanan tersebut. Contoh dari aplikasi Streaming Server adalah VLC dan Darwin Server.
Aplikasi streaming biasanya memiliki ekstensi *.tar.gz dan *.exe untuk diinstalasi. Masing-masing didukung oleh sistem operasi terentu. Aplikasi streaming *.tar.gz didukung oleh sistem operasi FreeBSD 5.2, Fedore 10.0, dan Red Hat, dalam proses instalasi. Sementara itu, sistem operasi Windows 2000 dan Windows XP mendukung instalasi aplikasi streaming berekstensi *.exe.

- Web Server

Ada dua buah pengertian mengenai web server, sebagai berikut:

- Sebuah komputer yang bertanggung jawab untuk menerima request HTTP dari clients dan menyediakan Web Pages serta objek-objek yang berkaitan dengannya.
- Sebuah program komputer yang berfungsi seperti yang telah dijelaskan pada point pertama.

- FTP Server

Penjelasan lebih lanjut dari FTP Server ini akan dijelaskan pada bagian selanjutnya dari modul ini.

- Proxy Server

Penjelasan lebih lanjut dari Proxy Server ini akan dijelaskan pada bagian selanjutnya dari modul ini.

- Database Server

Sebuah database server adalah program komputer yang menyediakan layanan basis data untuk program komputer atau komputer lain. Basis data kadang diperlukan untuk sebuah aplikasi client-server. DBMS (Database Management System) sering menyediakan jasa basis data pada model client-server untuk akses basis data.
Saat ini, banyak vendor-vendor yang menyediakan jasa pembuatan server khusus yang dapat memenuhi kebutuhan user dan mudah dalam dalam perawatan serta penambahan hardware baru. Vendor-vendor tersebut antara lain adalah sebagai berikut:

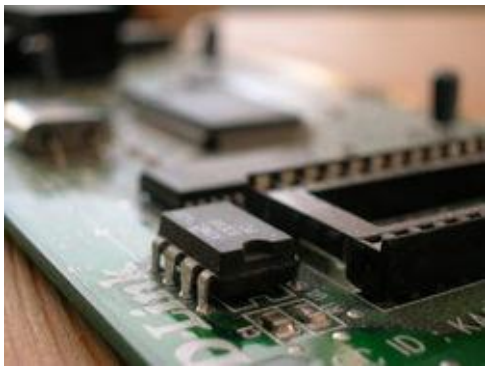
- ACER
- DELL
- EXTRON
- HP
- IBM

Komponen Jaringan

Di bawah ini akan dijelaskan lebih rinci beberapa komponen jaringan yang telah disebutkan di atas.

- Network Interface Card (NIC)

NIC adalah kartu jaringanyang berupa papan elektronik yang akan dipasang pada setiap komputer yang terhubung pada jaringan. Saat ini, banyak sekali jenis kartu jaringan. Akan tetapi, ada beberapa hal yang perlu diketahui dari kartu jaringan seperti tipe kartu, jenis protokol dan tipe kabel yang didukungnya.



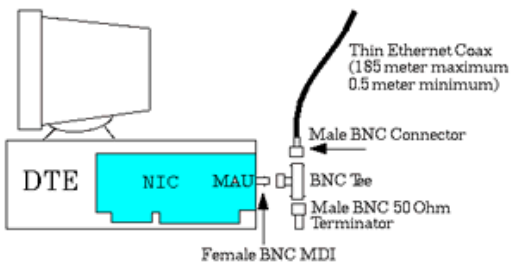
Gambar 1.3. Network Interface Card

Dengan perkembangan PC dan mainboard, maka tipe solt dan expansion slot pun bermacam-macam. Akan tetapi pada modul ini cukup dibahas mengenai ISA dan PCI. Ketika membeli komputer (khususnya komputer rakitan), tidak semua slot terisi. Slot yang kosong dapat digunakan untuk melakukan pemasangan kartu tambahan (mis: kartu suara, modem internal, atau kartu jaringan). Untuk membedakan slot ISA dan PCI tidak begitu sulit. Jika casing komputer dibuka, slot ISA biasanya berwarna hitam, sedangkan PCI berwarna putih. Untuk slot yang bewarna coklat umumnya adalah slot AGP.

Untuk protokol jaringan, ada beberapa protokol untuk sebuah kartu jaringan seperti Ethernet, Fast Ethernet, Token Ring, FDDI, dan ATM. Jenis Ethernet atau Fast Ethernet sering digunakan.

- 10Base2

10Base2 dikenal dengan thin ethernet karena menggunakan kabel koaksial jenis thin atau disebut dengan cheapernet. 10Base2 menggunakan topologi bus[1].

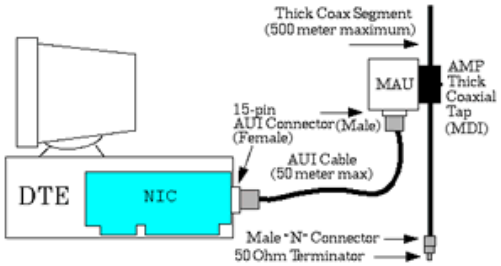


Gambar 1.4. Ethernet 10Base2

[1] Topologi bus akan dijelaskan pada bagian selanjutnya

- 10Base5

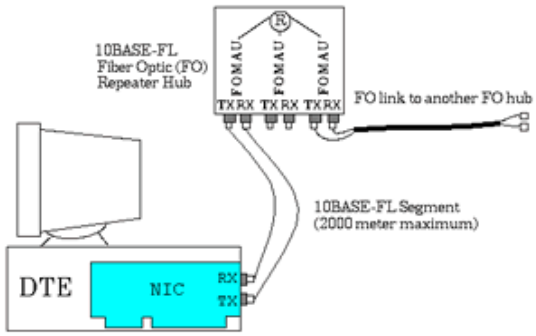
10Base5 dikenal dengan thick ethernet karena menggunakan kabel koaksial jenis thick. Topologi yang digunakan juga sama dengan 10Base2, yakni topologi bus.



Gambar 1.5. Ethernet 10Base5

- 10BaseF

10BaseF menggunakan serat optik. 10BaseF jarang digunakan karena biaya yang mahal dan pemasangannya yang sulit. Biasanya, jenis ini digunakan untuk penghubung (link) antarsegmen. Hal ini disebabkan kemampuan jaraknya yang dapat mencapai hingga 200 meter. Spesifikasi dari 10BaseF identik dengan 10BaseT.



Gambar 1.6. Ethernet 10BaseF

- 100BaseT

100BaseT disebut sebagai fast ethernet atau 100BaseX. Ethernet ini memiliki kecepatan 100Mbps. Ada beberapa tipe 100BaseT berdasarkan kabel yang digunakan.

  - 100BaseT4 memakai kabel UTP kategori 3, 4, atau 5. Kabel yang digunakan ada 4 buah
  - 100BaseTX, memakai kabel UTP kategori 5 dan kabel yang dipakai hanya dua pasang
  - 100BaseFX, menggunakan kabel serat optik

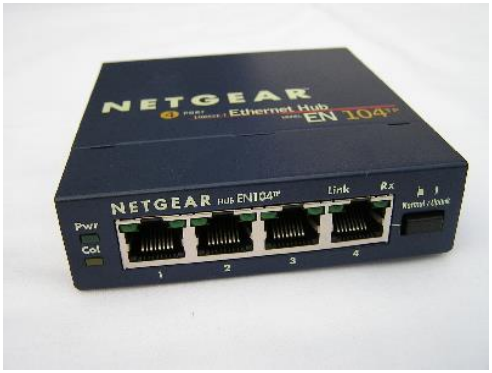
Pada 100BaseT yang menggunakan kabel koaksial, maksimum total panjang kabel yang menggunakan hub Class II yaitu 205 meter dengan 100 meter panjang segmen dan 5 meter adalah panjang kabel untuk menghubungkan hub ke hub. Sementara itu untuk 100BaseFX dengan menggunakan 2 repeater bisa mencapai 412 meter, dan panjang dengan serat optik dapat mencapai 2000 meter.

- 100VG-AnyLAN

100VG-AnyLAN bukan ethernet murni karena metode akses medianya berdasarkan demand priority. 100VG-AnyLAN bisa digunakan dengan sistem frame ethernet atau frame token ring.
Kabel yang digunakan adalah UTP kategori 3 atau 5. TIdak seperti ethernet biasa yang menggunakan kabel UTP panjang maksimum segmennta 100 meter, pada 100VG-AnyLAN jika yang dipakai adalah UTP kategori 5 maka panjang maksimum segmennya bisa sampai 150 meter, sedangkan yang memakai kabel serat optik panjang maksimum segmennya 2000 meter.

- Hub

Hub adalah suatu perangkat yang memiliki banyak port. Hub akan menghubungkan beberapa node (komputer) sehingga akan membentuk suatu jaringan dengan topologi star[2]. Pada jaringan yang umum, sebuah port akan menghubungkan hub dengan komputer Server. Sementara itu port yang lain digunakan untuk menghubungkan hub dengan node-node.



Gambar 1.7. Hub

Penggunaan hub dapat dikembangkan dengan mengaitkan suatu hub ke hub lainnya. Sedangkan dari segi pengelolaannya, HUB dibagi menjadi dua jenis, sebagai berikut:

- Hub manageable

Hub jenis ini bisa dikelola dengan software yang ada di bawahnya.

- Hub non-managable

Hub jenis ini pengelolaannya dilakukan secara manual.
Hub hanya memungkinkan user untuk berbagi jalur yang sama. Pada jaringan tersebut, tiap user hanya akan mendapatkan kecepatan dari bandwith yang ada. Misalkan jaringan yang digunakan adalah Ethernet 10 Mbps dan pada jaringan tersebut tersambung 10 unit komputer. Jika semua komputer tersambung ke jaringan secara bersamaan, maka bandwith yang dapat digunakan oleh masing-masing user rata-rata adalah 1 Mbps.

- Repeater

Repeater hampir sama seperti Hub. Repeater menggunakan topologi bus, yang bekerja memperkuat sinyal agar lalu lintas data dari workstation (client) ke server atau sebaliknya lebih cepat jika jaraknya semakin jauh. Dengan repeater ini, jaringan dan sinyal akan semakin kuat, apalagi jika kabel yang digunakan adalah jenis koaksial.

[2] Topologi star akan dijelaskan pada bagian selanjutnya

Gambar 1.8. Repeater

- Bridge (jembatan)

Bridge, sesuai dengan namanya, berfungsi menghubungkan beberapa jaringan yang terpisah, untuk jaringan yang sama maupun berbeda. Bridge memetakan alamat jaringan dan hanya memperbolehkan lalu lintas data yang diperlukan. Ketika menerima sebuah paket, bridge menentukan segmen tujuan dan sumber. Jika segmennya sama, maka paket akan ditolak. Bridge juga dapat mencegah pesan rusak agar tidak menyebar keluar dari suatu segmen.

- Switch

Switch dikenal juga dengan istilah LAN switch merupakan perluasan dari bridge. Ada dua buah arsitektur switch, sebagai berikut:

- Cut through

Kelebihan dari arsitektur switch ini terletak pada kecepatan, karena pada saat sebuah paket datang, switch hanya memperhatikan alamat tujuan sebelum diteruskan ke segmen tujuannya.

- Store and forward

Switch ini menerima dan menganalisa seluruh isi paket sebelum meneruskannya ke tujuan dan untuknya memerlukan waktu.
Keuntungan menggunakan switch adalah karena setiap segmen jaringan memiliki bandwith 10 Mbps penuh, tidak terbagi seperti pada hub.

Gambar 1.9. Switch

- VDSL

Very high-bit-rate Digital Subscriber Line port merupakan alat yang berguna sebagai converter dari label UTP ke kabel telepon. VDSL biasanya digunakan untuk menghubungkan jaringan LAN yang jaraknya kurang dari 500 meter. Untuk menggunakannya harus sepasang, satu dipasang di Switch atau Hub

yang berhubungan dengan server. Sedangkan yang satu lagi, dipasang di Switch atau Hub yang berhubungan dengan client.

- Wireless
  Ada bermacam-macam merk dan jenis dari wireless. Beberapa notebook sudah memasang wireless secara otomatis. Untuk memanfaatkan wireless yang sudah ada di komputer atau memasang sebagai kartu jaringan, user harus memiliki Hub atau Switch yang ada fasilitas wirelessnya.
- Router
  Cara kerja router mirip dengan switch dan bridge. Perbedaannya, router adalah penyaring atau filter lalu lintas data. Penyaringan dilakukan dengan menggunakan protokol tertentu. Router bukanlah perangkat fisikal, melainkan logikal. Misalnya sebuah IP router dapat membagi jaringan menjadi beberapa subnet sehingga hanya lalu lintas yang ditujukan untuk IP adress tertentu yang dapat mengalir dari suatu segmen ke segmen lainnya.

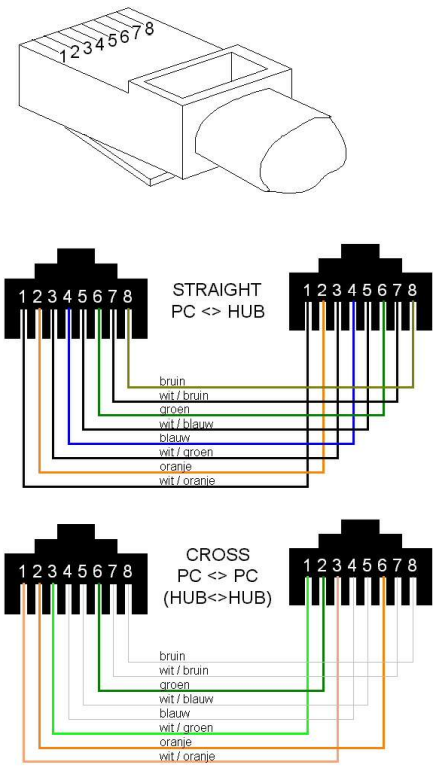
- Kabel jaringan
  Kabel jaringan yang biasanya digunakan untuk suatu jaringan antara lain adalah UTP (unshielded twisted pair), koaksial, dan serat optik. Sesuai dengan perkembangan Hub, penggunaan kabel UTP lebih sering dipilih. Hal ini dikarenakan harganya yang tidak mahal dan kemampuannya yang dapat diandalkan.

  - Twisted Pair Cable (UTP)

Ada dua buah jenis kabel UTP yakni shielded dan unshielded. Shielded adalah kabel yang memiliki selubung pembungkus. Sedangkan unshielded tidak memiliki selubung pembungkus. Untuk koneksinya digunakan konektor RJ11 atau RJ-45.

Gambar 1.10. Konektor RJ-45

UTP cocok untuk jaringan dengan skala dari kecil hingga besar. Dengan menggunakan UTP, jaringan disusun berdasarkan topologi star dengan hub sebagai pusatnya. Kabel ini umumnya lebih reliable dibandingkan dengan kabel koaksial. Hal ini dikarenakan Hub memiliki kemampuan dara error correction yang akan meningkatkan kecepatan transmisi.
Ada beberapa kategori dari kabel UTP. Yang paling baik adalah kategori 5. Ada dua jenis kabel, yakni straight-through dan crossed. Kabel Straight-through dipakai untuk menghubungkan komputer ke Hub, komputer ke Switch atau Switch ke Switch. Sedangkan kabel crossed digunakan untuk menghubungkan Hub ke Hub atau Router ke Router. Untuk kabel kategori 5, ada 8 buah kabel kecil di dalamnya yang masing-masing memiliki kode warna. Akan tetapi hanya kabel 1,2,3,6. Walaupun demikian, ke delapan kabel tersebut semuanya terhubung dengan jack.
Untuk kabel straight-through, kabel 1, 2, 3, dan 6 pada suatu ujung juga di kabel 1,2,3, dan 6 pada ujung lainnya. Sedangkan untuk kabel crossed, ujung yang satu adalah kebalikan dari ujung yang lain (1 menjadi 3 dan 2 menjadi 6).



Gambar 1.11. Kabel UTP

- Kabel koaksial

Media ini paling banyak digunakan sebagai media LAN, meski lebih mahal dan lebih sukar dibanding dengan UTP. Kabel ini memiliki bandwith yang lebar, oleh karena itu dapat digunakan untuk komunikasi broadband. Ada dua buah jenis kabel koaksial, sebagai berikut:

a. Thick Coaxial

Kabel jenis ini digunakan untuk kabel pada instalasi Ethernet antar gedung. Kabel ini dapat menjangkau jarak 500 m bahkan sampai 2500 m dengan memasang repeater.

b. Thin Coaxial

Kabel jenis ini cocok untuk jaringan rumah atau kantor. Kabel ini mirip seperti kabel antenna TV, harganya tidak mahal, dan mudah dipasangnya. Untuk memasangnya, kabel ini menggunakan konektor BNC. Pada jaringan jenis ini, untuk melakukan sambungan ke masing-masing komputer menggunakan konektor T.

- Serat Optik

Jaringan yang menggunakan F/O biasanya digunakan pada perusahaan besar. Hal ini disebabkan karena mahal dan pemasangannya sulit. Akan tetapi, jaringan dengan media ini memiliki kehandalan yang sangat baik dan kecepatan yang sangat tinggi (sekitar 100 Mbps). Keunggulan lainnya adalah bebas dari gangguan lingkungan. Pembahasan mengenai serat optik ini akan dibahas secara lebih rinci pada bagian selanjutnya.

- Kabel Telepon

Kabel telepon adalah media yang digunakan untuk LAN beberapa tahun terakhir. Kabel ini biasanya digunakan untuk menghubungkan jaringan antar gedung. Kabel telepon yang digunakan untuk diluar gedung ini biasanya

dilengkapi dengan 3 kawat, dimana 2 kawat digunakan untuk penghubung data, sementara yang satu lagi digunakan untuk mencegah agar kawat-kawat tidak putus jika dibentang. Konektor untuk kabel telepon adalah RJ-11

Pemilihan Kabel

Pada bagian sebelumnya, telah disinggung mengenai beberapa jenis kabel jaringan. Pada bagian ini akan dibahas cara memilih jenis kabel.

Biasanya, kabel yang sudah tertanam tidak akan diangkat atau dipindahkan selain dalam keadaan terpaksa. Oleh karena itu, perlu dilakukan sebuah perencanaan untuk menentukan jenis kabel yang akan digunakan. Suatu kendala akan terjadi, jika terjadi kesalahan dalam pemilihan kabel.

Apabila akan membangun suatu jaringan, tentukan jenis dan kualitas kabel yang baik sehingga dapat membuat jaringan berjalan dengan baik hingga 10 tahun atau lebih. Selain jenis, masalah kecepatan dan jarak akses data perlu diperhitungkan.

Di bawah ini adalah beberapa jenis kabel jaringan, kecepatan, jarak, dan konektor yang digunakan.

Tabel 1.1 : Kabel Jaringan berdasarkan kecepetan, jarak, dan konektor

Tipe	Kecepatan	Jarak	Konektor
UTP Kategori 5	10 Mbps	± 300 kaki	RJ45
Kabel koaksial	10 Mbps	± 2500 kaki	BNC Connector
Kabel Telepon			Konverter RJ11
Wireless	lebih dari 10 Mbps	Tergantung jenis dan merek	
Serat Optik	100 Mbps	± 3 mil	ST (spring loaded twist)

Topologi Jaringan

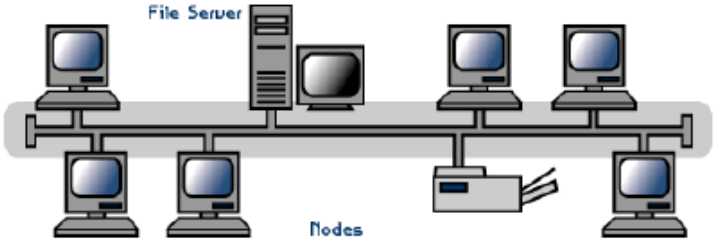
Setelah kita mengetahui komponen untuk membangun sebuah jaringan, maka langkah selanjutnya adalah merancang jaringan sesuai yang kita perlukan. Apakah jaringan yang akan kita bangun akan berbentuk garis lurus (*bus*), bintang (*star*), lingkaran (*ring*), dan sebagainya. Hal tersebut dinamakan dengan topologi jaringan.

Secara fisik, topologi jaringan dapat berupa topologi bus, ring, star ataupun campuran.

Topologi Bus

Jaringan dengan topologi ini disebut juga dengan linear bus karena dihubungkan hanya melalui satu kabel yang linier. Kabel yang umum digunakan adalah kabel koaksial. Pada awal dan akhir kabel digunakan terminator.

Contoh: Jaringan yang menggunakan kartu penghubung jaringan ethernet 10Base2

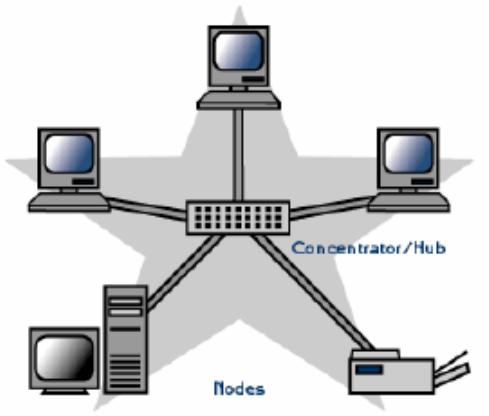


Gambar 1.12. Topologi Bus

Topologi Star

Jaringan dengan teknologi ini berbentuk seperti bintang. Hubungan antar node diperantari dengan menggunakan hub atau concentrator. Tiap node dihubungkan dengan kabel ke hub.

Contoh: Jaringan yang memakai ethernet 10BaseT, membangun jaringan dengan menggunakan manageable switch.

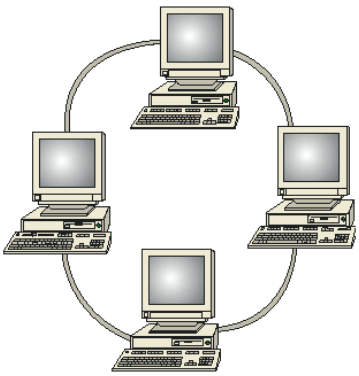


Gambar 1.13. Topologi Star

Topologi Ring

Pada topologi ini setiap node saling berhubungan dengan node lainnya sehingga membentuk ring.

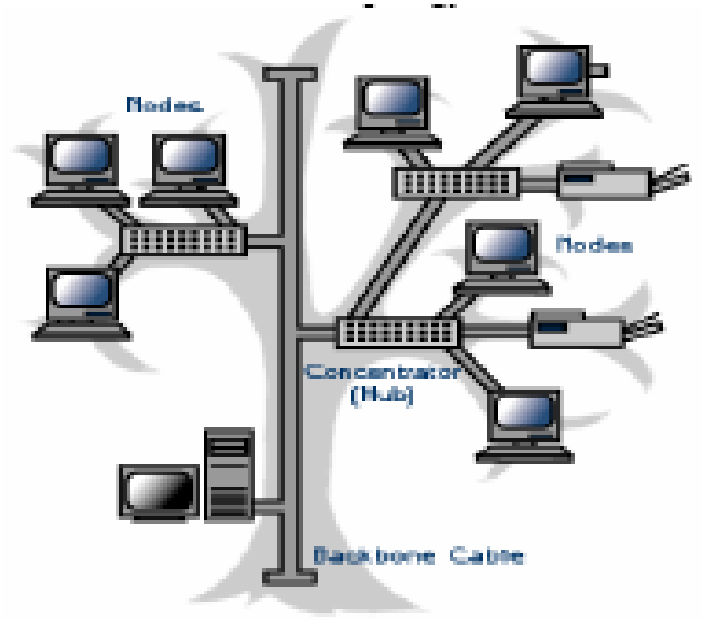
Contoh: Jaringan yang menggunakan FDDL



Gambar 1.14. Topologi Ring

Topologi Tree

Topologi tree ini merupakan gabungan dari kombinasi tiga topologi yang ada. Beberapa pihak juga menyebut dengan topologi mesh.



Gambar 1.15. Topologi Tree

Topologi Logik

Secara logik, jaringan dibedakan atas bagaimana data dilewatkan melalui jaringan. Ada dua buah topologi logik, yakni:

- Bus

Sistem ini menggunakan metode broadcast ke jaringan untuk komunikasi data dari node ke node. Tiap node akan menerima broadcast ini dan aakn diabaikan jika memang bukan tujuannya.

- Ring

Sistem ini menggunakan metode token-passing dimana data yang dikirim akan berputar dari node ke node sampai node tujuan ditemukan.

Pemilihan Topologi

Pada saat pemilihan topologi jaringan, cukup banyak pertimbangan yang harus diambil tergantung pada kebutuhan. Faktor-faktor yang perlu mendapatkan pertimbangan antara lain adalah sebagai berikut:

- Biaya, sistem apa yang paling efisien yang dibutuhkan organisasi
- Kecepatan, sejauh mana kecepatan yang dibutuhkan oleh sistem
- Lingkungan, mis: listrik, adakah faktor lingkungan yang berpengaruh
- Ukuran (skalabilitas), berapa besar ukuran jaringan. Apakah jaringan memerlukan file server atau sejumlah server khusus.

Konektivitas, apakah pemakai yang lain perlu mengakses jaringan dari berbagai lokasi.

Tabel di bawah ini menunjukkan keuntungan dan kerugian dari masing-masing topologi.

Tabel 1.2 : Keuntungan dan Kerugian Topologi Jaringan

Topologi	Keuntungan	Kerugian
BUS	Hemat Kabel Layout kabel sederhana Mudah dikembangkan Tidak butuh kendali pusat Mudah untuk menambah maupun mengurangi terminal	Deteksi dan isolasi kesalahan sangat kecil. Kepadatan lalu lintas tinggi. Keamanan data kurang terjamin Kecepatan akan menurun bila pemakai bertambah Diperlukan repeater untuk jarak jauh.
RING	Hemat kabel Dapat melayani lalu lintas datayang padat	Peka kesalahan Pengembangan jaringan lebih kaku. Kerusakan pada termina dapat melumpuhkan kerja seluruh jaringan Lambat, karena pengiriman menunggu giliran token
STAR	Fleksibel karena pemasangan kabel mudah Penambahan atau pengurangan terminal mudah Kontrol terpusat sehingga memudahkan deteksi dan isolasi kesalahan dalam pengelolaan jaringan	Boros kabel Kontrol terpusat (Hub) jadi elemen kritis.

Perangkat Lunak

Operasi sistem yang digunakan dalam jaringan bermacam-macam. Yang paling populer adalah Linux dan Microsoft Windows. Dalam modul ini, perangkat lunak yang digunakan lebih dititiberatkan kepada Microsoft Windows.

Jika ingin membuat sebuah jaringan Workgroup, dapat menggunakan sistem operasi Windows 95, Windows 98, atau Windows ME. Untuk lebih baiknya, direkomendasikan untuk menggunakan sistem operasi Windows XP atau Windows 2000 Server. Untuk sistem operasi server. Lebih baik lagi jika menggunakan Microsoft Windows Server 2003. Dengan sistem operasi tersebut, seseorang telah dapat merancang jaringan LAN.

Ada beberapa fitur yang harus dimiliki sebuah sistem operasi untuk server, sebagai berikut:

- Realtime

Artinya adalah sistem operasi harus mendukung aplikasi yang realtime.

- Security

Artinya adalah sistem operasi harus memiliki fitur keamanan untuk mencegah penyerangan atau penyalahgunaan pihak luar.

- Reliabilitas

Artinya adalah sistem operasi harus dapat beroperasi 24 jam sehari 7 hari seminggu 365 hari setahun tanpa gangguan.

- Skalabilitas

Artinya adalah, jika diperlukan penambahan kemampuan maka sistem operasi harus mampu melakukan upgrade hardware seperti prosesor, memori, hard disk.

Meski Microsoft Windows unggul dalam GUI (grafis), akan tetapi ada beberpa kelemahan sistem operasi server ini, antara lain sebagai berikut:

- Implementasi untuk sistem keamanan masih sangat rendah, sehingga rentan terkena serangan dari luar
- Lisensi Microsoft sangat mahal dan akan bertambah mahal jika ada penambahan node.
- API Windows selalu bertambah di setiap versinya, setiap ada perubahan pada API-nya menyebabkan beberapa aplikasi tidak berjalan.

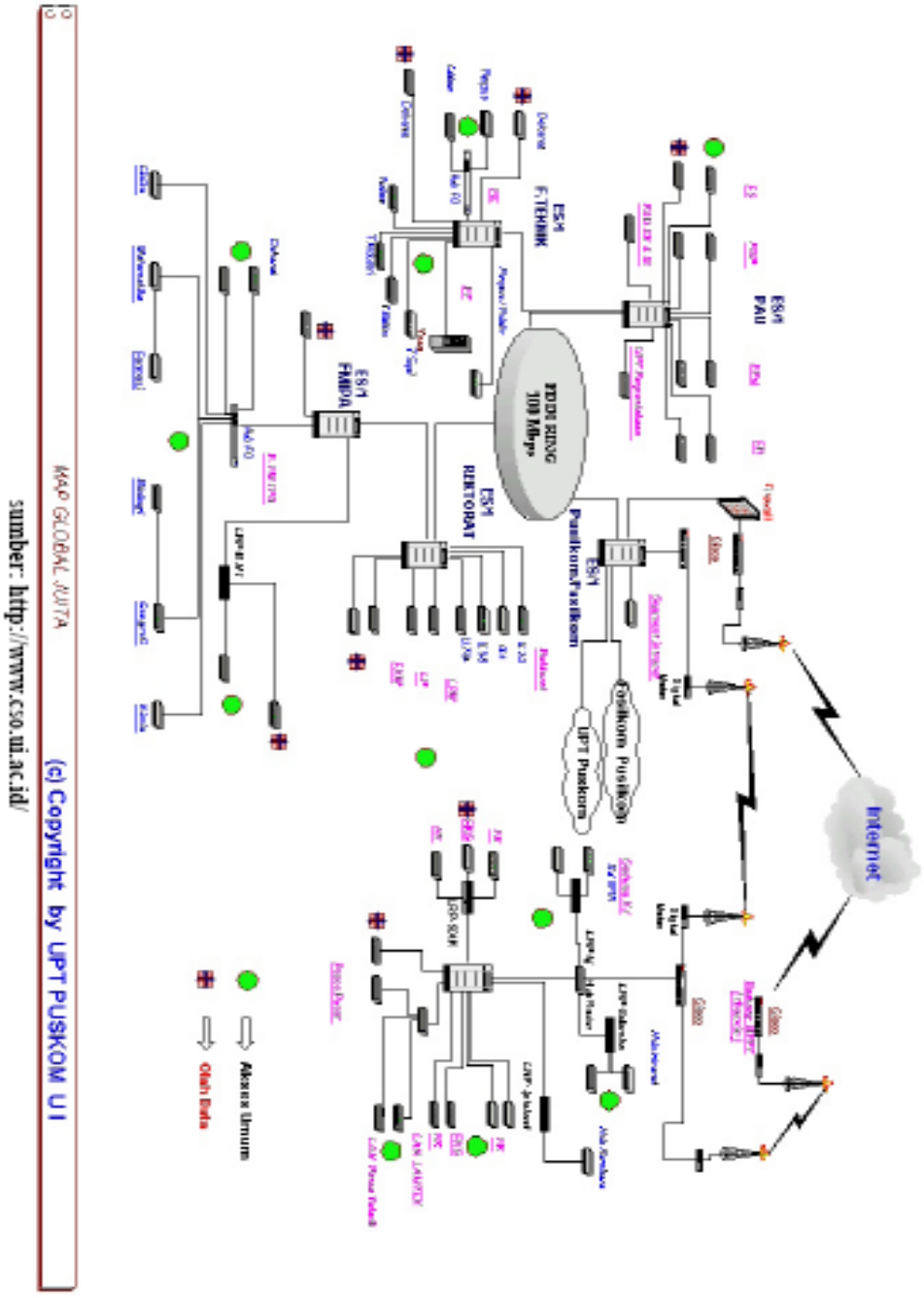
Sedangkan Linux memiliki beberapa kelebihan untuk dijadikan sistem operasi server, antara lain sebagai berikut:

- Linux memiliki lisensi gratis
- Dukungan vendor aplikasi terhadap linux semakin meningkat
- Linux bersifat portabel, dapat berjalan di semua platform komputasi yang ada
- Linux relatif lebih aman dan stabil karena didukung adanya komunitas open source untuk hal ini.

PERANCANGAN LAN

Contoh dalam merancang sebuah LAN, diambil dari Jaringan UI Terpadu (JUITA)

Gambar 1.16. Contoh Rancangan LAN



Seperti dapat terlihat pada gambar sebelumnya, jaringan JUITA menggunakan beberapa topologi jaringan. Sebagai backbone (jaringan utama), dibangun pada FDDI Ring 100Mbps. Untuk menghubungkan ke client, ada mesin ES/1 yang digunakan untuk router. Kondisi di lapangan tidak memungkinkan semua mesin ES/1 terhubung langsung ke FDDI Ring. Untuk itu mesin ES/1 yang tidak terhubung dengan backbone menggunakan mesin ES/1 lainnya untuk melakukan penghubungan ke backbone.

Dari masing-masing mesin ES/1 kemudian dihubungkan dengan menerapkan topologi star ke masing-masing gedung. Sementara itu sambungan masing-masing topologi star ini menggunakan topologi linear bus.

Dengan memanfaatkan kabel FiberOptik sebagai sarana koneksi, dari mesin ES/1 ditarik beberapa buah kabel. Dari kabel-kabel tersebut, ada yang berfungsi untuk kabel utama, namun ada juga yang digunakan untuk kabel

cadangan. Kabel-kabel tersebut kemudian dihubungkan ke hub utama (menggunakan converter serat optik). Dari hub utama, untuk menghubungkan dengan gedung lain (yang melewati *outdoor space*), digunakanlah kabel serat optik. Jadi hubungan dari mesin ES/1 ke hub ke gedung lain melalui adapter di main hub. Jika masih ada gedung lain, maka digunakan serat optik dengan sumber koneksi dari gedung terdekat.
Dari masing-masing Hub utama, dihubungkan dengan hub lainnya menggunakan topologi star. Alasan utama dalam pemilihan serat optik untuk ruangan luar adalah untuk mengurangi akibat dari serangan petir. Hal ini dikarenakan wilayah UI Depok sangatlah rawan terhadap serangan petir.
Dari contoh di atas dapat diambil suatu kesimpulan bahwa dalam membuat perancangan jaringan LAN (mis: diagram jalur pengkabelan), harus disesuaikan dengan beberapa faktor seperti kondisi fisik user (perusahaan) seperti lokasi user dalam lingkungan kerja dan kondisi ruangan perusahaan.

Persiapan
Persiapan yang dimaksudkan di sini adalah menyiapkan dan menyediakan semua hal yang dibutuhkan untuk instalasi, termasuk pengaturan ruangan untuk komputer client dan penempatannya.

Prosedur Instalasi
Persiapan yang baik meliputi dua buah prosedur, sebagai berikut:
- Konstruksi
- Elektris

Beberapa peralatan yang dibutuhkan untuk melakukan pemasangan jaringan adalah sebagai berikut:
- Obeng belimbing dan obeng minus
- Obeng belimbing bermagnet
- Test pen
- Tang pemotong
- Pinset
- Tang penjepit (*clipper* atau *crampper*)
- Solder listrik + timah jika diperlukan
- Multi tester
- Kapas bertangkai (*cotton bud*)
- Tester untuk mengetahui konetisitas kabel UTP jika ada.

Kabel yang belum dipasang (baik dengan konektor maupun tidak) akan lebih baik jika telah diberi label sebelumnya. Hal ini akan memudahkan orang yang masih awam terhadap jaringan untuk memilih kabel sendiri dengan tepat jika dibutuhkan. Selain itu, pelabelan dapat mempercepat pemilihan kabel dalam jumlah yang besar (tidak perlu repot meneliti satu per satu).
Sebelum dilakukan instalasi perlu dibuat sebuah jadwal pekerjaan yang baik agar proses instalasi berjalan dengan lancar. Jadwal tersebut secara sekuensial (urut) meliputi hal-hal berikut:
- Membuat desain jaringan di atas kertas sesuai dengan kondisi nyata di lapangan
- Melakukan pembongkaran dan pembenahan infrastruktur lapangan,
- Melakukan pemasangan peralatan jaringan secara menyeluruh
- Melakukan konfigurasi peralatan jaringan secara menyeluruh
- Menguji konektivitas semua node dalam jaringan

Tim Instalasi

Tim instalasi adalah orang-orang yang terlibat dalam melaksanakan instalasi suatu jaringan LAN. Orang-orang ini hendaknya bukanlah orang-orang sembarangan, melainkan memenuhi kriteria-kriteria sebagai berikut:

- Memiliki pengalaman dalam bidang jaringan komputer, khususnya pengalaman dalam melakukan instalasi jaringan
- Sehat secara fisik, dalam artian tidak memiliki catat fisik yang tidak dapat memenuhi persyaratan dalam proses instalasi jaringan.
- Sehat secara mental dan jiwa.

Dalam menentukan jumlah anggota tim yang efisien sesuai dalam melakukan instalasi jaringan harus memperhatikan beberapa faktor sebagai berikut:

- Luas lokasi instalasi
- Kapasitas user jaringan yang diperlukan
- Besar biaya yang akan dikeluarkan untuk proses penginstalan jaringan

Sebelum melakukan instalasi, ada beberapa hal yang harus dilakukan tim instalasi. Hal-hal tersebut adalah sebagai berikut:

- Menjaga konsentrasi pada saat instalasi dengan makan makanan yang cukup
- Menggunakan perlengkapan pelindung badan
- Memeriksa daya guna alat-alat konstruksi dengan saksama.
-

Penempatan Server

Ruangan yang digunakan untuk menyimpan atau menempatkan server sebaiknya dipasangi pendingin udara (AC). Selain itu, server sebaiknya diletakkan di tempat yang aman, dan tidak mudah dijangkau oleh orang yang tidak memiliki hak atau mengerti tentang jaringan.

Switch atau Hub sebaiknya diletakkan dekat Server, bahkan jika mungkin dibuatkan rak agar rapi. Modem harus disimpan berdekatan dengan server dan jalur telepon.

Berikut ini adalah komponen yang harus berada di ruangan server:

- Komputer Server
- Switch atau Hub
- Modem ADSL atau Modem DialUp
- Jalur Telepon
- Komputer untuk memantau aktivitas jaringan
- Printer
- Scanner jika diperlukan

Penempatan Workstation

Pengaturan komputer yang digunakan sebagai workstation atau client tidak terlalu ketat seperti halnya penempatan server. Komputer workstation dapat diletakkan sesuai dengan kebutuhannya.

Pengkabelan

Sebelum melakukan instalasi atau pemasangan kabel, dilakukan pemeriksaan terhadap kabel yang akan dipasang. Pemeriksaan ini dilakukan baik untuk kabel urus maupun kabel UTP. Hal ini bertujuan untuk mengetahui kabel yang tidak dapat digunakan (mis: karena isinya terputus).

Setelah kabel dipasang, gunakan pipa penutup agar rapi. Pemberian tanda pada kabel sebaiknya diterapkan agar memudahkan pengawasan ataupun perbaikan jika terjadi suatu kerusakan.
Setelah komputer diletakkan di masing-masing lokasi, maka langkah selanjutnya adalah menarik kabel, memasang kartu jaringan, memasang konektor RJ45, dan sebagainya.
Untuk memasang kabel, harus berangkat dari ruangan server. Dengan kata lain, semua ujung kabel diratakan di ruangan server dekat dengan Hub. Misalkan memasang dan menarik kabel untuk 20 unit PC dan sisanya untuk server dan workstation di ruangan server. Tarik satu per satu kabel dan sesuaikan dengan keinginan, dengan perincian sebagai berikut:

- Panjang kabel UTP dari Hub ke Server maksimal 8 meter
- Panjang kabel UTP dari Hub ke Workstation di ruangan server maksimal 12 meter
- Panjang kabel UTP dari Hub ke Workstation di ruangan lainnya maksimal 100 meter.

Dapat diketahui bahwa sistem pengkabelan di Indonesia belum terdesain dengan baik, hal ini terbukti karena kabel-kabel jaringan yang terinstal tidak berada dalam suatu dinding atau tembok dan berkeliaran bebas hingga dapat mengganggu aktivitas harian.

Pemasangan Konektor

Seseorang yang ingin memasang konektor harus mengetahui susunan kabel yang akan dipasang. Asal sama ujung ke ujung bisa saja, akan tetapi cara ini tidak tepat. Harus diperhatikan warna-warnanya. Untuk lebih jelasnya ikuti langkah-langkah berikut ini:

- Potong kabel UTP dan kupas bagian luarnya dengan menggunakan tang pemotong.
- Susun urutan warna sesuai dengan ketentuan berikut.

Untuk kabel straight through, maka posisi warnanya untuk satu konektor ke konektor lain ditampilkan pada tabel berikut:

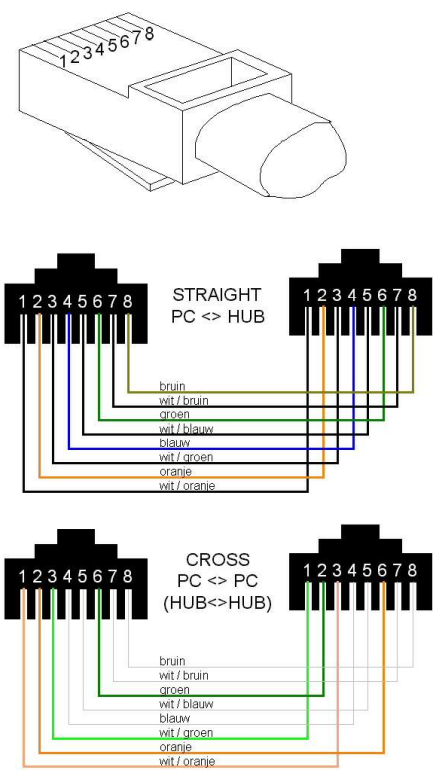
Putih Orange		Putih Orange
Orange		Orange
Putih Hijau		Putih Hijau
Biru		Biru
Putih Biru		Putih Biru
Hijau		Hijau
Putih Coklat		Putih Coklat
Coklat		Coklat

- Untuk kabel cross, maka posisi warnanya untuk satu konektor ke konektor lain ditampilkan pada tabel berikut:

Putih Orange		Putih Hijau
Orange		Hijau
Putih Hijau		Putih Orange
Biru		Biru
Putih Biru		Putih Biru
Hijau		Orange
Putih Coklat		Putih Coklat
Coklat		Coklat

- Siapkan konektor RJ-45 dan masukkan kabel. Setiap ujung konektor posisinya harus sama. Selain itu, bagian luar atau pembungkus kabel harus tejenpit agar kokoh dan tidak goyang.
- Setelah kabel masuk dan rata sampai ujung konektor, masukkan konektor dan jepit dengan tang clipper.
- Lakukan dengan hati-hati agar tidak ada konektor yang meleset.
- Lakukan hal yang sama untuk ujung kabel. Ingat ketentuan warnanya.

Jika ingin melakukan instalasi kabel pada dinding, soket RJ-45 dapat ditanamkan pada dinding kayu, plester, maupun beton



Gambar 1.17. Pemasangan Konektor

Pemasangan kartu jaringan

Pada modul ini akan dicontohkan pemasangan kartu jaringan ke dalam salah satu soket PCI di komputer. Ikuti langkah-langkah berikut:

- Buka casing komputer, baik untuk Server maupun untuk workstation
- Setelah casing terbuka, pasang (tancapkan) kartu jaringan ke soket atau slot PCI di komputer.
- Pasang mur di bagian atas sehingga kartu jaringan kokoh dan tidak goyang.
- Setelah selesai tutup casing dan rapikan letak komputer yang sudah dipasang kartu jaringan
- Tancapkan kabel yang telah dipasang konektor RJ45 ke port di Hub dan di komputer.

Dalam membangun jaringan ini sebaiknya melibatkan ahli teknik atau bangunan. Perhatikan pula fakotr petir di lingkungan tersebut, Dan sebaiknya memasang grounding di komputer server.

Pemasangan VDSL

Memasang VDSL pada dasarnya sama seperti memasang Hub atau Switch, sehingga tidak begitu sulit. Akan tetapi dalam memasang VDSL diperlukan dua jenis kabel, yakni kabel telepon (RJ11) dan kabel UTP (RJ45).
Ikuti langkah-langkah berikut untuk memasang VDSL master maupun client.

- Pastikan ruang server telah ada. Hal ini disebabkan semua VDSL harus dipasang di ruangan pusat.
- Pasang kabel telepon yang menghubungkan 2 gedung atau lebih
- Setelah kabel terpasang, pastikan master VDSL dipasang di ruang Server sedangkan yang satunya lagi dipasang di ruang Client atau Workstation yang ada di gedung lain.
- Pasang kabel telepon dari port yang tersedia. Gunakan konektor RJ11 atau dapat pula menggunakan kabel yang biasanya digunakan untuk telepon, baik untuk master VDSL maupun Client.
- Pasang konektor UTP. Baik pada master VDSL, mapun pada client.
- Tancapkan kabel telepon ke port line pada master VDSL.
- Tancapkan kabel UTP yang sudah dibuat pada master VDSL, dan satunya lagi tancapkan pada Hub atau Switch.
- Lakukan hal yang sama untuk VDSL client.
- Tancapkan kabel power pada port yang tersedia, baik untuk master VDSL, mapun untuk client.

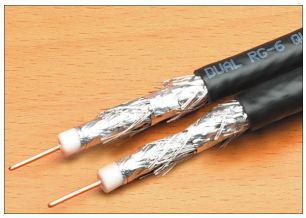
Jika dilihat dari penjelasan yang telah diberikan sebelumnya, VDSL harus sepasang dan tidak dapat berdiri sendir (master VDSL dan client). Keduanya dihubungkan dengan kabel telepon. Sementara itu master VDSL dihubungkan ke Sitwch utama, dan VDSL client dihubungkan ke switch untuk didistribusikan ke komputer yang akan dihubungkan dalam jaringan.
Tahapan selanjutnya adalah melakukan pengaturan VDSL. Biasanya terdapat CD instalasi yang harus dilakukan pada komputer sever maupun komputer client. Ikuti tahapan-tahapan yang ada di dalamnya.

BAB 2
Memasang Kabel UTP dan BNC pada Jaringan

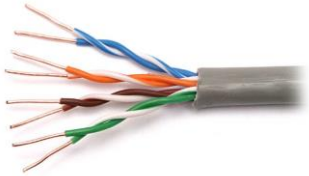
2.1 Jaringan Komputer Pada Saat Ini

Pada zaman teknologi informasi yang telah maju seperti saat ini, jaringan komputer merupakan sebuah hal yang sudah umum digunakan oleh banyak orang, bahkan mungkin dapat dikatakan bahwa jaringan komputer merupakan sebuah hal yang telah menjadi keharusan bagi sebagian besar bagi para pengguna komputer. Jaringan komputer yang ada pada saat ini pada umumnya lebih banyak menggunakan media kabel (wired) daripada menggunakan media nirkabel (wireless). Hal ini dikarenakan beberapa kelebihan dari media kabel bila dibandingkan dengan media nirkabel, yaitu dalam hal kecepatan transmisi data serta keamanan dari data yang dikirimkan. Pada saat ini terdapat beberapa media yang diklasifikasikan sebagai media kabel (wired) dalam arsitektur network, antara lain :

- Kabel Coaxial



- Kabel UTP (Unshielded Twisted Pair)



- Kabel STP (Shielded Twisted Pair)

- Kabel SSTP (Screened Shielded Twisted Pair)

- Kabel FO (Fiber Optic)

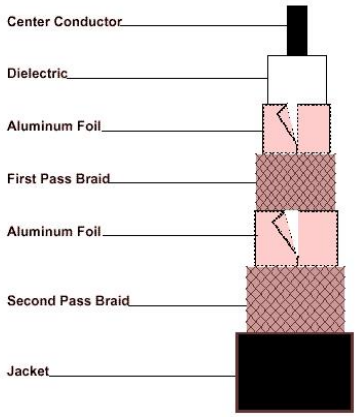
Dari semua media yang telah disebutkan di atas, hanya terdapat 2 media yang sangat lazim digunakan pada jaringan komputer saat ini, yaitu menggunakan media kabel coaxial serta kabel UTP sebagai penghubung antara komputer yang satu dengan yang lainnya sehingga terbentuk suatu jaringan yang saling menghubungkan antara komputer yang satu dengan yang lainnya.Jika dilihat secara lebih mendalam, sebenarnya antara UTP, STP dan SSTP memiliki kesamaan dari jenis kabelnya, yaitu sama-sama terdiri atas 4 pasang kabel yang terdiri atas warna putih orange, orange, putih hijau, hijau, putih biru, biru dan putih coklat, coklat.

Yang membedakan dari ketiga media tersebut hanyalah pada bagian pelindungnya, dimana UTP tidak memliki pelindung sama sekali, sedangkan STP memiliki pelindung

berupa lapisan isolator yang terdiri dari serabut-serabut kabel berlapiskan perak pada bagian kabelnya dan SSTP pada dasarnya memiliki isolator yang sama halnya dengan STP tetapi ditambah lagi dengan isolator pada setiap pasang pilinan kabelnya. Semua isolator tersebut berguna untuk menghindari terjadinya interferensi elektromagnetik, namun dengan adanya isolator tersebut maka akibatnya harga dari kabel tersebut menjadi lebih mahal bila dibandingkan dengan UTP sehingga banyak orang lebih menggunakan UTP daripada STP atau SSTP. Sedangkan kabel fiber optic jarang digunakan dengan alasan konektor yang tidak terlalu universal dan biayanya sangat mahal sekali bila dibandingkan dengan media lainnya, menyebabkan kabel fiber optic sangat jarang digunakan dan lebih sering digunakan hanya sebagai kabel *untuk backbone* dikarenakan kecepatan transmisi datanya yang sangar cepat dan terbebas dari gangguan interferensi elektromagnetik. Atas dasar hal tersebut, modul ini akan difokuskan untuk membahas lebih dalam lagi mengenai 2 jenis media yang lebih umum digunakan tersebut, yaitu kabel coaxial dan kabel UTP.

Kabel Coaxial

Kabel coaxial pada awalnya banyak dikenal orang sebagai kabel untuk digunakan pada kalangan radio amatir serta banyak digunakan pula sebagai kabel televisi. Kabel coaxial merupakan media kabel yang digunakan pertama kali dalam jaringan komputer sehingga pada saat ini kabel coaxial semakin jarang digunakan dan telah tergantikan oleh kabel UTP, tetapi masih banyak pula jaringan komputer yang menggunakan kabel coaxial sebagai media untuk transmisi data di dalam jaringan komputer, terutama jaringan yang masih menggunakan topologi jaringan berupa linier/bus dan ring. Yang perlu diingat adalah bahwa kabel coaxial sudah tidak digunakan lagi sebagai standar bagi media kabel dalam jaringan komputer. Kabel coaxial memiliki konektor bernama BNC yang merupakan singkatan dari British Naval Connector.



Kabel coaxial terdiri atas:

- sebuah konduktor yang terbuat tembaga
- lapisan pembungkus dengan sebuah kawat yang berfungsi sebagai ground bagi kabel
- sebuah lapisan yang terbuat dari karet yang berfungsi sebagai lapisan paling luar dari kabel coaxial

Saat ini terdapat dua kategori kabel coaxial yang digunakan sebagai media bagi jaringan komputer, yaitu kabel thin coaxial (10 Base 2) dan kabel thick coaxial (10 Base 5), berikut adalah perbedaan antara kabel thin coaxial dengan kabel thick coaxial :

Kabel thin coaxial

Kabel thin coaxial (RG/U-58) ini merupakan jenis kabel yang banyak dipergunakan di kalangan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Agar dapat dipergunakan sebagai perangkat jaringan maka kabel coaxial jenis ini harus memenuhi standar IEEE 802.3 10BASE2, dimana diameter rata-rata berkisar 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Setiap perangkat yang terhubung pada jaringan komputer dihubungkan dengan konektor BNC T. Kabel jenis ini juga dikenal sebagai thin Ethernet atau ThinNet.

Kabel coaxial jenis ini, jika diimplementasikan dengan konektor T dan terminator dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

- Pada setiap ujung kabel diberi terminator 50-ohm. (diharapkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar)
- Panjang maksimal kabel adalah 185 meter per segment.

- Pada setiap segment maksimum koneksi terhadap perangkat jaringan adalah 30 perangkat.
- Kartu jaringan cukup menggunakan transceiver yang onboard, tidak perlu tambahan transceiver, kecuali untuk repeater.
- Maksimum ada 3 segment terhubung satu sama lain.
- Setiap segment sebaiknya dilengkapi dengan satu ground.
- Panjang minimum antar T-Connector adalah 0.5 meter.
- Maksimum panjang kabel dalam satu segment adalah 555 meter.

Kabel Thick coaxial

Kabel thick coaxial (RG/U-8) merupakan kabel yang dispesifikasikan berdasarkan standar IEEE 802.3 10BASE5, dimana kabel ini mempunyai diameter rata-rata 12mm, dan biasanya diberi warna kuning; kabel jenis ini biasa disebut sebagai standard ethernet atau thick Ethernet, atau hanya disingkat ThickNet, atau bahkan cuma disebut sebagai yellow cable.

Kabel Coaxial ini jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

- Pada setiap ujung diberi terminator 50-ohm (diharapkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).
- Maksimum 3 segment dengan peralatan terhubung atau berupa populated segments.
- Setiap kartu jaringan mempunyai pemancar tambahan.
- Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini repeaters.
- Maksimum panjang kabel per segment adalah sekitar 500 meter.
- Maksimum jarak antar segment adalahsekitar 1500 meter.
- Setiap segment harus diberi ground.
- Jarak maksimum antara tap atau pencabang dari kabel utama ke perangkat adalah sekitar 5 meter.
- Jarak minimum antar tap adalah sekitar 2,5 meter.

Kabel thin coaxial digunakan untuk menggantikan keberadaan kabel thick coaxial (thick coaxial tidak digunakan lagi untuk LAN modern). Kabel thin coaxial tidak direkomendasikan lagi, tetapi masih digunakan pada jaringan LAN yang sangat kecil.

Keuntungan dari kabel coaxial :

- Tidak membutuhkan support dari peralatan elektronik lainnya (tidak membutuhkan hub/switch, dll)
- Kecil dan fleksibel sehingga memudahkan untuk dipasang

Kerugian dari kabel coaxial :

- Harganya mahal
- Sulit untuk melakukan perubahan jika telah terpasang pada jaringan
- Sulit untuk melakukan diagnosa permasalahan
- Jika satu komputer mengalami down, maka semua jaringan akan mengalami down pula, hal ini dikarenakan topologi jaringan yang digunakan oleh kabel coaxial adalah topologi bus/linier dan ring
- Tidak tahan lama

Bila dibandingkan antara kabel coaxial dan kabel UTP, maka terdapat perbedaan, yaitu :

- Hanya dapat berjarak maksimum 185 meter anatara komputer yang pertama dan terakhir
- Hanya dapat menampung maksimum 30 komputer pada sebuah segmen
- Harga dari kabelnya lebih mahal

Kabel UTP

Pada saat ini, kabel UTP (Unshielded Twisted Pair) merupakan salah satu jenis kabel yang paling banyak digunakan dalam jaringan komputer. Sesuai dengan namanya, kabel ini merupakan sebuah kabel yang berisi empat pasang kabel tembaga yang tiap pasangnya dipilin. Tujuan dari kabel yang terpilin tersebut adalah untuk mengurangi kelemahan yang ada pada kabel UTP terhadap gangguan (noise) elektris, baik itu yang berasal dari dalam kabel yaitu pengaruh interferensi antar kabel (crosstalk) dan dari luar kabel yaitu interferensi elektromagnetik (EMI) dan interferensi frekuensi radio (RFI). Kabel ini tidak dilengkapi dengan pelindung (unshielded) seperti yang ada pada STP atau SSTP. Keempat pasang kabel (delapan kabel) yang menjadi isi kabel berupa kabel tembaga tunggal yang berisolator. Kode kabel UTP adalah 10 Base T atau 100 Base T.
Hingga saat ini terdapat tujuh kategori kabel UTP yang umum digunakan, yaitu kabel UTP kategori satu sampai dengan kategori tujuh seperti yang terlihat pada tabel di bawah ini :

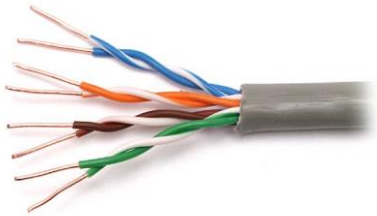
Cable	Type	Feature
Type CAT 1	UTP	analog (biasanya digunakan di perangkat telephone pada umumnya dan pada jalur ISDN –integrated service digital networks. Juga untuk menghubungkan modem dengan line telepon).
Type CAT 2	UTP -	up to 1 Mbits (sering digunakan pada topologi *token ring*)
Type CAT 3	UTP / STP	16 Mbits data transfer (sering digunakan pada topologi *token ring* atau 10BaseT)
Type CAT 4	UTP, STP	20 Mbits data transfer (biasanya digunakan pada topologi *token ring*)
Type CAT 5	UTP, STP - up to 100 MHz	100 Mbits data transfer / 22 db
Type CAT 5enhanced	UTP, STP - up to 100 MHz	1 Gigabit Ethernet up to 100 meters - 4 copper pairs (kedua jenis CAT5 sering digunakan pada topologi *token ring 16Mbps*, *Ethernet* 10Mbps atau pada *FastEthernet 100Mbps*)
Type CAT 6	up to 155 MHz or 250 MHz	2,5 Gigabit Ethernet up to 100 meters or 10 Gbit/s up to 25 meters . 20,2 db (*Gigabit Ethernet*)
Type CAT 7	up to 200 MHz or 700 Mhz	Giga-Ethernet / 20.8 db (*Gigabit Ethernet*)

Kategori yang diberikan kepada setiap UTP merupakan spesifikasi untuk masing-masing kabel tembaga dan juga untuk konektor pada masing-masing ujung kabel tersebut. Masing-masing seri merupakan revisi dari seri UTP yang telah ada sebelumnya. Revisi tersebut merupakan perbaikan atas kualitas kabel, kualitas pembungkusan kabel (isolator) dan juga untuk kualitas pilinan untuk masing-masing pasang kabel. Selain itu juga untuk menentukan besarnya frekuensi yang dapat melewati kabel tersebut, dan juga kualitas isolatorsehingga dapat menekan efek induksi antar kabel (noise dapat ditekan seminimal mungkin).

Kabel UTP CAT1 dan CAT2 tidak digunakan dalam jaringan komputer karena kemampuan transfer datanya sangat rendah. Kabel UTP CAT1 dan CAT2 ini banyak digunakan untuk komunikasi telepon, atau berfungsi sebagai kabel telepon pada umumnya. Sedangkan untuk jaringan komputer digunakan kabel UTP CAT3 sampai CAT7. Kabel UTP CAT3 dapat digunakan untuk komunikasi dengan kecepatan hingga mencapai 10 Mbps. Kabel UTP CAT5 dapat dipergunakan untuk jaringan dengan kecepatan hingga mencapai 100 Mbps dan oleh sebab itulah kabel UTP jenis ini merupakan kabel yang paling umum serta banyak digunakan pada jaringan komputer yang menggunakan kabel UTP. Spesifikasi antara CAT5 dan CAT5 enchanced (CAT5e) mempunyai standar industri yang sama, namun pada CAT5e telah dilengkapi dengan

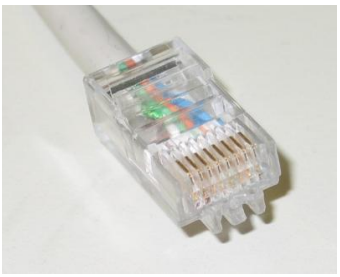
insulator untuk mengurangi efek induksi atau electromagnetic interference. Kabel CAT5e dapat digunakan untuk menghubungkan network hingga kecepatan 1Gbps.

UTP CAT5 / CAT5e



Pasangan kabel pertama adalah : putih biru - biru
Pasangan kabel kedua adalah : putih orange- orange
Pasangan kabel ketiga adalah : putih hijau - hijau
Pasangan kabel keempat adalah : putih coklat - coklat

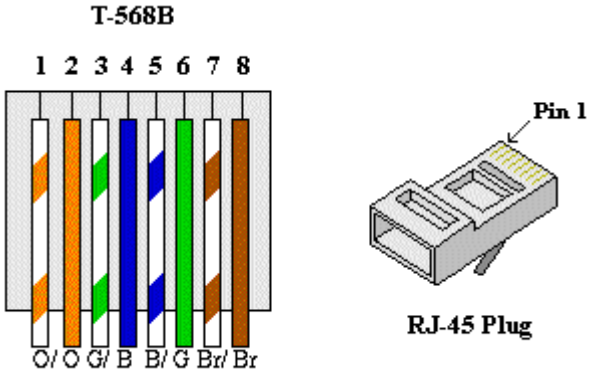
Konektor yang digunakan untuk kabel UTP CAT5 adalah RJ-45. (Terlihat pada gambar di bawah)



Untuk digunakan dalam jaringan, dikenal 2 buah tipe penyambungan kabel UTP ini, yaitu kabel straight, kabel crossover dan kabel rollover. Setiap jenis koneksi ini memiliki fungsi yang berbeda satu sama lain, straight cable digunakan untuk menghubungkan antara client dan hub/switch/router atau hub/switch dan router (pada intinya, kabel ini digunakan untuk menghubungkan peralatan yang berbeda jenisnya) . Crossover cable digunakan untuk menghubungkan antara client dan client atau digunakan untuk menghubungkan hub/switch dan hub/switch (pada intinya, kabel ini digunakan untuk menghubungkan peralatan yang sama jenisnya).

Kabel Straight

Untuk jenis kabel straight, pada intinya adalah menghubungkan kabel dengan warna yang sama antara ujung yang satu dengan yang lainnya (misalnya biru disambungkan dengan biru, putih orange disambungkan dengan putih orange), tetapi ada standard yang biasa dipakai di asia yaitu EIA/TIA-568B.



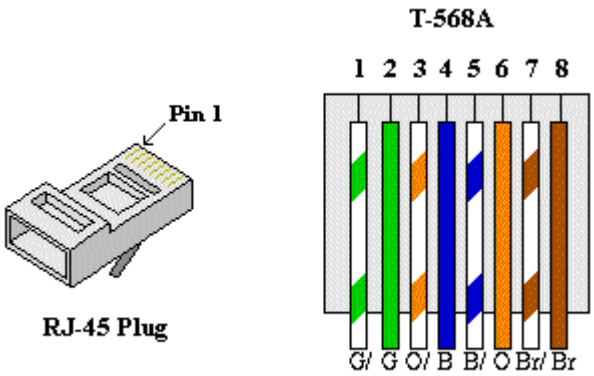
Seperti yang terlihat pada gambar :

- Pin nomor 1 merupakan kabel berwarna putih orange
- Pin nomor 2 merupakan kabel berwarna orange
- Pin nomor 3 merupakan kabel berwarna putih hijau
- Pin nomor 4 merupakan kabel berwarna biru
- Pin nomor 5 merupakan kabel berwarna putih biru
- Pin nomor 6 merupakan kabel berwarna hijau
- Pin nomor 7 merupakan kabel berwarna putih coklat
- Pin nomor 8 merupakan kabel berwarna coklat

Jadi, untuk membuat koneksi kabel straight sesuai standar yang ada, maka pada kedua ujung kabel sama-sama menggunakan urutan EIA/TIA-568B untuk urutan pengkabelannya.

Kabel crossover

Untuk jenis kabel crossover, ada standard yang biasa dipakai di asia yaitu EIA/TIA-568A. Standard EIA/TIA-568A membalikkan koneksi pasangan kabel berwana orange dan hijau yang ada pada EIA/TIA-568B , sehingga pasangan kabel berwarna biru dan orange menjadi 4 pin yang berada di tengah.



Seperti yang terlihat pada gambar :

- Pin nomor 1 merupakan kabel berwarna putih hijau
- Pin nomor 2 merupakan kabel berwarna hijau
- Pin nomor 3 merupakan kabel berwarna putih orange
- Pin nomor 4 merupakan kabel berwarna biru
- Pin nomor 5 merupakan kabel berwarna putih biru
- Pin nomor 6 merupakan kabel berwarna orange
- Pin nomor 7 merupakan kabel berwarna putih coklat
- Pin nomor 8 merupakan kabel berwarna coklat

Jadi, untuk membuat koneksi kabel cross sesuai standar yang ada, maka pada sebuah ujung kabel menggunakan urutan EIA/TIA-568B untuk urutan pengkabelannya dan pada ujung yang lainnya menggunakan urutan EIA/TIA-568A untuk urutan pengkabelannya

Kelebihan dari kabel UTP :

- Teknologi yang paling umum digunakan sehingga banyak orang mengetahuinya
- Menggunakan kabel yang sangat murah bila dibandingkan dengan media kabel lainnya
- Mudah untuk melakukan penginstalasian
- Tidak terjadi gangguan pada komputer lain dalam jaringan jika terdapat satu komputer yang mengalami permasalahan, hal ini disebabkan oleh topologi jaringan yang digunakan oleh UTP berbentuk star (bintang).

Kekurangan dari kabel UTP :

- Dapat terkena interferensi elektromagnetik maupun interferensi frekuensi radio
- Memiliki keterbatasan jarak

Bila dibandingkan antara kabel UTP dan kabel coaxial, maka terdapat perbedaan, yaitu :

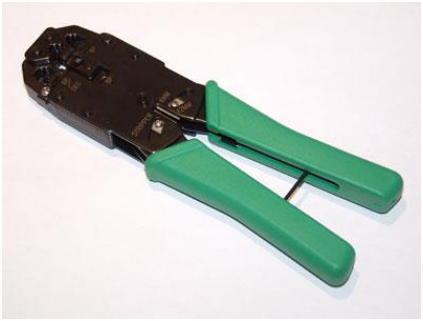
- Panjang maksimal kabel UTP untuk dapat bekerja secara optimal adalah kurang dari 100 meter dan panjang minimal kabel UTP untuk dapat bekerja secara optimal adalah lebih dari 2 meter.
- Harga dari kabel UTP lebih murah daripada kabel coaxial
- Jaringan yang menggunakan kabel UTP harus menggunakan hub/switch sedangkan dengan menggunakan kabel coaxial, hal tersebut tidak perlu dilakukan karena terdapat BNC Tee)

2.2 Bahan dan peralatan yang perlu dipersiapkan untuk memasang kabel UTP

1. Crimping Tool

Crimping Tool 1

Crimping Tool 2



Crimping Tool 3

Crimping Tool 4

Crimping tool merupakan alat yang berfungsi untuk memasang konektor RJ-45 pada kabel UTP. Pada beberapa crimping tool, selain digunakan untuk memasang konektor RJ-45, dapat pula digunakan untuk memasang konektor RJ-11 maupun RJ-22. Crimping tool yang ada saat ini memiliki bentuk yang bermacam-macam mulai dari yang kecil (hanya memiliki fungsi untuk mengcrimping RJ-45) hingga yang besar (dapat memotong, mengupas kabel dan mengcrimping berbagai jenis konektor). Seperti terlihat pada gambar ada beberapa contoh dari crimping tool, namun yang umum digunakan di Indonesia adalah crimping tool yang pertama dan yang ketiga. Disarankan untuk menggunakan crimping tool yang cara kerja crimpingnya adalah menekan (seperti pada crimping tool yang ketiga dan keempat) karena memiliki hasil yang lebih baik bila dibandingkan dengan crimping tool yang cara kerjanya seperti tang (crimping tool yang pertama dan kedua).

2. Network Tester

Network Tool 1

Network Tool 2

Network Tool 3

Network tester adalah alat yang digunakan untuk mengecek konektivitas kabel utp yang telah berhasil dicrimping atau kabel coaxial yang telah dipasangi oleh konektor bnc. Untuk kabel utp, terdapat 2 network tester, yaitu network tester yang dapat untuk dipisah (pada umumnya digunakan untuk mengecek konektivitas kabel yang jauh atau kabel yang telah terpasang) dan network tester yang tidak dapat

dipisah (digunakan untuk mengecek wiring map kabel yang baru dibuat). Network tester yang dapat dipisah umumnya menggunakan lampu led untuk mengecek konektivitas tiap kabel yang terpasang sedangkan network tester yang tidak dapat dipisah umumnya menggunakan sistem digital dalam pengecekannya. Pada gambar di atas, network tester yang dapat dipisah tampak pada gambar nomor 1 dan 2, sedangkan network tester yang tidak dapat dipisah tampak pada gambar nomor 3.

3. Tone Generator

Tone Generator 1

Tone Generator 2

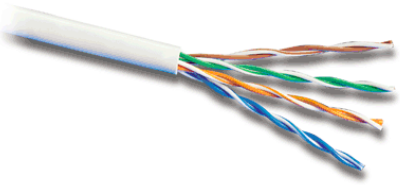
Tone generator adalah alat yang digunakan untuk melakukan tracing (pendeteksian) pada posisi manakah kabel LAN tersebut putus, alat ini sangat berguna pada kabel-kabel yang telah terpasang sehingga tidak perlu melakukan penggantian pada seluruh kabel hanya perlu melakukan

penggantian pada sebagian atau penyambungan ulang pada kabel yang putus tersebut.

4. Konektor RJ-45

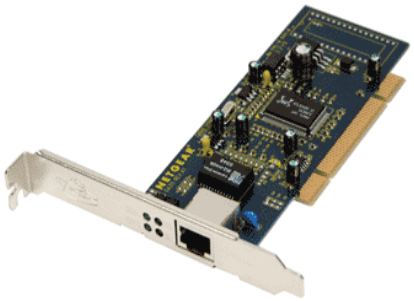
Konektor RJ-45 berfungsi untuk menghubungkan antara kabel LAN (CAT 5e atau CAT 6) dengan LAN Card. Pada umumnya konektor RJ-45 ini bermerk AMP. Pada ujung konektor ini terdapat tembaga yang berfungsi sebagai konduktor antara inti kabel dengan konduktor pada LAN Card.

5. Kabel UTP



Kabel UTP (Unshielded Twisted Pair) merupakan salah satu media koneksi antara satu peralatan dengan peralatan lainnya dengan menggunakan perantara media kabel tembaga. Misalnya antara komputer dengan switch atau antar switch. Penjelasan lebih lanjut mengenai kabel UTP terdapat pada bagian atas dari modul ini.

6. LAN Card UTP



LAN card (disebut juga NIC – Network Interface Card) merupakan salah satu perangkat keras yang dibutuhkan komputer agar komputer dapat terhubung dengan jaringan. LAN card dapat berupa perangkat yang terpisah dari motherboard atau dapat juga sudah tergabung di motherboard (*built in*). LAN card didesain sedemikian sehingga mempunyai MAC address yang unik, artinya tidak ada dua LAN card yang mempunyai MAC address yang sama.LAN card yang paling sering digunakan pada saat ini adalah LAN card UTP. LAN card UTP adalah perangkat keras komputer yang digunakan sebagai media perantara untuk menghubungkan kabel UTP dengan komputer. Dengan memasukan ujung kabel UTP (yang telah dibungkus oleh konektor RJ – 45) ke dalam LAN card, komputer dapat terhubung dengan suatu jaringan sehingga memungkinkan untuk berkomunikasi dengan komputer lain yang ada dalam jaringan tersebut.

2.3 Bahan dan peralatan yang perlu dipersiapkan untuk memasang kabel coaxial

1. Konektor BNC

Konektor BNC adalah konektor yang digunakan sebagai terminal dari kabel coaxial. Konektor BNC ini digunakan untuk menghubungkan kabel coaxial dengan LAN card yang mendukung adanya konektor BNC.

2. BNC Terminator 50 Ohm

BNC Terminator 50 Ohm berfungsi sebagai terminal penutup dalam rangkaian jaringan yang menggunakan kabel coaxial. Alat ini digunakan untuk menutup port dari passive hub yang tidak digunakan, passive hub adalah konektor dengan 4 port menggunakan konektor jenis BNC, yang digunakan sebagai pusat perkabelan yang datang dari workstation. Port yang tidak terpakai harus di terminate.

3. Konektor T (Tee) BNC

Konektor TEE BNC merupakan gabungan dari 3 konektor BNC. Konektor ini mempunyai bentuk menyerupai huruf T. Konektor BNC bisa berupa gabungan 3 konektor BNC yang sejenis (female maupun male) ataupun kombinasi antara konektor BNC male dan female. Pada gambar di samping, dicontohkan konektor BNC dengan kombinasi 2 konektor BNC female (terdapat pada ujung kanan dan kiri) dan satu konektor BNC male (terdapat pada tengah – tengah). Kegunaan dari konektor TEE BNC ini adalah sebagai terminal dari kabel coaxial dengan daya tampung yang

lebih banyak daripada konektor BNC biasa. Digunakan untuk menghubungkan antar kabel coaxial dan menghubungkan kabel coaxial dengan LAN card BNC

4. Kabel Coaxial

Kabel coaxial terdiri dari dua buah konduktor. Pusatnya berupa inti kawat padat yang dibalut dengan sekat dan dililiti lagi oleh kawat berselaput konduktor. Jenis kabel ini biasa digunakan untuk jaringan dengan bandwidth tinggi. Berdasarkan ukuranya, kabel coaxial terdiri dari dua jenis :

- **Kabel coaxial gemuk (*thick coaxial cable*)**

Kabel coaxial gemuk biasa disebut sebagai standard ethernet atau *thick Ethernet* (disingkat : ThickNet). Kabel ini mempunyai diameter sekitar 12 mm dan biasa diberi warna kuning. Karena warnanya yang kuning ,maka kabel ini juga disebut *yellow cable*. Pada ujung kabel ini diterminasi dengan BNC terminator 50 ohm. ThickNet dapat menjangkau sejauh 500 meter. Thicknet menggunakan spesifikasi Ethernet 10 base 5.

Kelebihan :

- Interferensi *noise* kecil
- Jangkauan lebih luas
- Mampu menampung sampai 100 jaringan (termasuk repeater)

Kekurangan :

Mahal dan sulit penginstalannya

- **Kabel coaxial kurus (*thin coaxial cable*)**

Kabel ini banyak dipergunakan pada radio amatir. Akan tetapi dapat juga digunakan dalam jaringan dengan syarat memenuhi standard IEEE 802.3 10 base 2. Diameter kabel ini kira – kira 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Kabel ini juga disebut sebagai *thin Ethernet* atau ThinNet. Setiap ujung kabel diberi terminator 50 ohm. ThinNet hanya dapat menjangkau sampai 185 meter.

Kelebihan :

Murah dan mudah dalam instalasinya

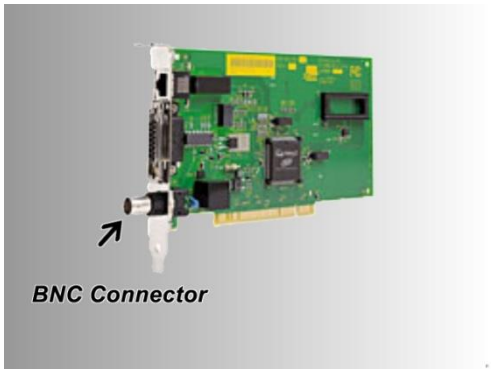
Kekurangan :

- Interferensi noise besar
- Jangkauan sempit
- Hanya dapat menampung 30 komputer

5. BNC Network Tester

Network tester adalah alat yang digunakan untuk mengecek konektivitas kabel utp yang telah berhasil dicrimping atau kabel coaxial yang telah dipasangi oleh konektor bnc. Untuk kabel coaxial, hanya terdapat 1 jenis network tester, yaitu network tester yang dapat dipisah (pada umumnya digunakan untuk mengecek konektivitas kabel yang jauh atau kabel yang telah terpasang). Network tester yang dapat dipisah umumnya menggunakan lampu led untuk mengecek konektivitas kabel yang terpasang. Pada gambar di atas, tampak gambar BNC network tester yang dapat dipisah

6. Lan Card dengan konektor BNC



LAN card BNC mempunyai komponen yang sama dengan LAN card UTP. Perbedaan utamanya, LAN card UTP dia menghubungkan kabel UTP dengan komputer sedangkan LAN card BNC menghubungkan kabel coaxial dengan komputer. Dengan perbedaan kabel tersebut, maka penghubung yang ada pada kedua LAN card itu menjadi berbeda pula. LAN card UTP mempunyai lubang dengan bentuk yang kompatibel dengan RJ45 sedangkan LAN card BNC menggunakan konektor BNC yang memang kompatibel dengan kabel coaxial. Dengan memasukan ujung kabel coaxial yang telah diberi konektor BNC ke dalam konektor BNC pada LAN card maka komputer akan dapat terhubung dalam suatu jaringan sehingga memungkinkan untuk berkomunikasi dengan komputer lain yang ada dalam jaringan tersebut.

2.4 Memasang Desain Kabel Sesuai dengan Jaringan

Pemilihan jenis kabel

Dalam perancangan suatu jaringan, pemilihan jenis kabel merupakan hal yang sangat krusial karena kabel merupakan komponen utama dari suatu jaringan. Kabel yang ada dalam jaringan biasanya tertanam dan jarang diangkat atau dipindahkan kecuali terpaksa. Maka, jaringan yang dibangun diharapkan mampu berjalan baik selama 10 tahun atau lebih.

Topologi jaringan ada banyak macam, namun ada tiga yang utama yaitu linear bus, star dan ring. Selain dari jarak dan kecepatan akses, jenis topologi jaringan juga mempengaruhi jenis kabel yang dipakai. Oleh karena itu, sebelum menentukan jenis

kabel yang dipakai, sekiranya perlu memperhatikan jenis topologi dari jaringan yang akan dibangun.

Topologi Linear Bus

Jenis topologi ini menggunakan prinsip penggunaan media secara bersama – sama.Artinya semua node terhubung dalam media komunikasi data yang sama. Topologi ini menggunakan metode *broadcast* ke jaringan untuk komunikasi data dari node ke node. Maksudnya jika node A ingin mengirim suatu data pada node B di dalam topologi linear bus yang terdiri dari node A,B,C,D maka data dari A itu akan dikirim ke semua node. Setiap node akan menerima data dari *broadcast* A . Jika data itu bukan ditujukan untuk node itu maka data itu akan diabaikan oleh node tersebut. Dalam kasus ini, B,C,D akan menerima data dari A. Namun yang akan benar – benar menerima data adalah B. C dan D mengabaikan data tersebut karena memang tidak ditujukan untuk mereka. Broadcast yang berlebihan akan mengurangi kinerja dari jaringan. Oleh karena itu perlu adanya metode *switching* untuk mengurangi *broadcast.*

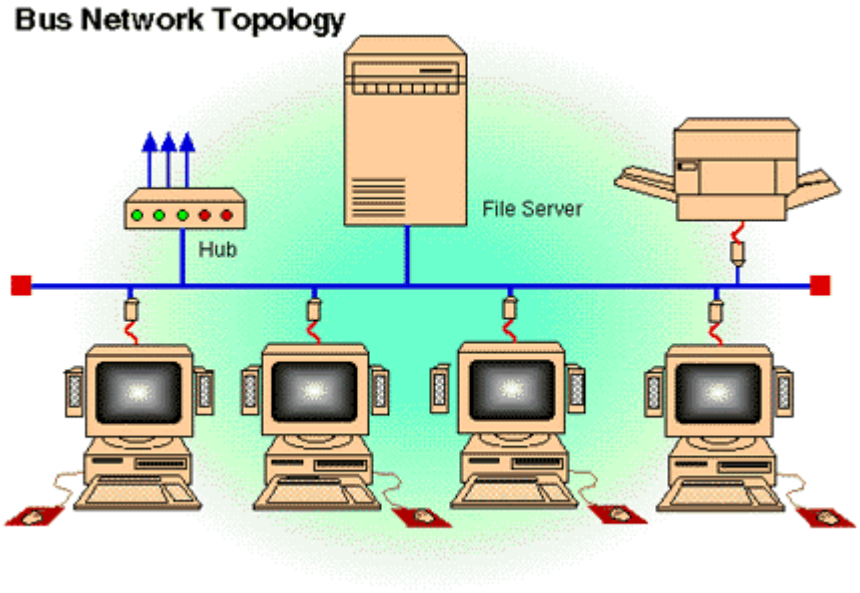
Topologi bus ini merupakan topologi yang banyak digunakan di awal penggunaan jaringan komputer karena topologi yang paling sederhana dibandingkan dengan topologi lainnya. Jika komputer dihubungkan antara satu dengan lainnya dengan membentuk seperti barisan melalui satu single kabel maka sudah bisa disebut menggunakan topologi bus.

Dalam topologi ini dalam satu saat, hanya satu komputer yang dapat mengirimkan data yang berupa sinyal elektronik ke semua komputer dalam jaringan tersebut dan hanya akan diterima oleh komputer yang dituju. Karena hanya satu komputer saja yang dapat mengirimkan data dalam satu saat maka jumlah komputer sangat berpengaruh dalam unjuk kerja karena semakin banyak jumlah komputer, semakin banyak komputer akan menunggu giliran untuk bisa mengirim data dan efeknya unjuk kerja jaringan akan menjadi lambat. Sinyal yang dikirimkan oleh satu komputer akan dikirim ke seluruh jaringan dari ujung satu sampai ujung lainnya.

Jika sinyal diperbolehkan untuk terus menerus tanpa bisa di interrupt atau dihentikan dalam arti jika sinyal sudah sampai di ujung maka dia akan berbalik arah, hal ini akan mencegah komputer lain untuk bisa mengirim data, karena untuk bisa mengirim data jaringan bus mesti bebas dari sinyal-sinyal. Untuk mencegah sinyal bisa terus menerus

aktif (bouncing) diperlukana adanya terminator, di mana ujung dari kabel yang menghubungkan komputer-komputer tersebut harus di-terminate untuk menghentikan sinyal dari bouncing (berbalik) dan menyerap (absorb) sinyal bebas sehingga membersihkan kabel tersebut dari sinyal-sinyal bebas dan komputer lain bisa mengirim data.

Dalam topologi bus ada satu kelemahan yang sangat menganggu kerja dari semua komputer yaitu jika terjadi masalah dengan kabel dalam satu komputer (ingat topologi bus menggunakan satu kabel menghubungkan komputer) misalnya kabel putus maka semua jaringan komputer akan terganggu dan tidak bisa berkomunikasi antar satu dengan lainnya atau istilahnya 'down'. Begitu pula jika salah satu ujung tidak diterminasi, sinyal akan berbalik (bounce) dan seluruh jaringan akan terpengaruh meskipun masing-masing komputer masih dapat berdiri sendiri (stand alone) tetapi tidak dapat berkomunikasi satu sama lain.



Jenis kabel yang digunakan pada topologi ini adalah kabel coaxial. Perangkat jaringan dihubungkan dengan menggunakan TEE connector. Pada ujung network diterminasi dengan terminator 50 ohm. Kesulitan utama dari penggunaan kabel coaxial ini adalah sulit untuk mengukur kabel coaxial agar cocok. Kalau tidak diukur dengan benar maka akibatnya dapat merusak NIC yang dipergunakan dan kinerja jaringan menjadi terhambat, tidak optimal. Topologi ini juga bisa menggunakan kabel fiber optic.

Kelebihan topologi linear bus :

- Mudah untuk menambahkan komputer atau peralatan lain ke jaringan
- Memerlukan kabel yang lebih sedikit dibandingkan dengan topologi star

Kekurangan :

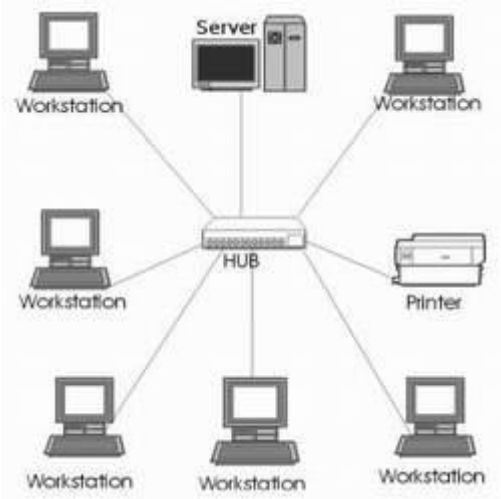
- Seluruh jaringan akan tidak dapat berjalan jika ada kerusakan pada kabel utama
- Terminator diperlukan pada kedua ujung dari kabel backbone
- Jika terlalu jauh maka diperlukan repeater untuk menguatkan sinyal

Topologi Star

Secara fisik, topologi ini berbentuk seperti bintang di mana pusatnya berupa konsentrator (hub atau switch). Semua node yang tergabung harus terhubung dengan konsentrator tersebut. Metode komunikasi yang digunakan sama dengan metode pada topologi bus yaitu broadcast. Jika menggunakan hub maka data akan dikirim ke semua node dan node yang bukan tujuan akan mengabaikan data tersebut. Jika menggunakan switch maka broadcast akan dihilangkan dan data akan dikirim hanya pada node tujuan saja.

Topologi ini paling banyak digunakan dalam jaringan komputer saat ini. Topologi ini awalnya digunakan dalam sistem mainframe. Jaringan star memberikan manajemen sumber daya (resource) secara sentral, namun dibandingkan dengan jenis bus, star ini memerlukan lebih banyak kabel karena tiap komputer dihubungkan ke hub, semakin banyak jumlah komputer yang akan dihubungkan ke jaringan maka semakin banyak pula kabel dan port yang ada di hub.

Kelemahan dari star ini juga adalah jika terjadi masalah dengan hub maka seluruh aktivitas jaringan akan ikut terganggu. Namun jika salah satu kabel terputus yang menghubungkan komputer dengan hub, maka yang mengalami masalah hanyalah pada komputer tersebut saja, komputer lain tetap dapat saling berkirim data (bandingkan dengan bentuk bus di atas).



Jenis kabel yang digunakan pada topologi ini adalah kabel UTP (biasanya CAT5). Namun tidak menutup kemungkinan untuk menggunakan kabel coaxial ataupun fiber optik.

Kelebihan :

- Mudah dibangun
- Dapat menambah atau mengurangi peralatan (device) tanpa mengganggu jaringan yang sudah ada
- Mudah untuk mendeteksi bagian kerusakan yang ada

Kekurangan :

- Memerlukan kabel yang lebih panjang dibandingkan dengan topologi linear bus
- Jika konsentrator (hub atau switch) mengalami kerusakan maka node yang tergabung dalam konsentrator tersebut tidak dapat berfungsi
- Lebih mahal dikarenakan biaya penambahan pada konsentrator
- Kabel dipasang sesuai dengan beberapa peraturan, antara lain jarak minimal dengan kabel listrik, jarak minimal kabel, diameter gulungan, dll
- Kabel jaringan dilindungi dari gangguan fisik lingkungan , antara lain menggunakan ducking, dll

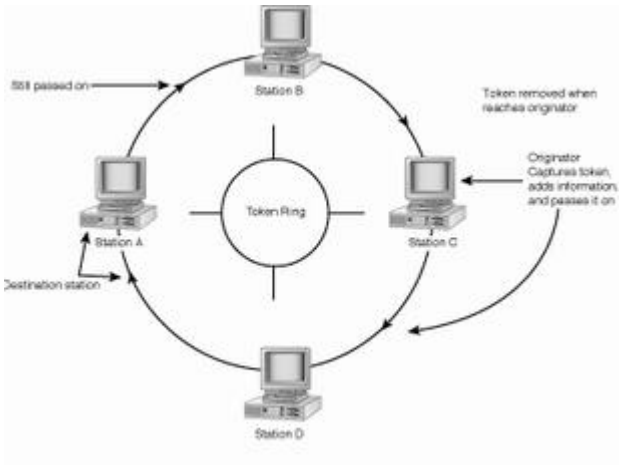
Topologi Ring

Topologi ring menghubungkan komputer dalam satu bentuk lingkaran kabel. Sinyal yang dikirim akan berkeliling dalam satu arah dan melalui tiap komputer. Tiap komputer dalam topologi ring ini akan berfungsi juga sebagai repeater (penguat sinyal) dan

mengirimkan sinyal ke komputer di sebelahnya. Karena tiap sinyal melalui tiap komputer, maka jika satu komputer mengalami masalah dapat berpengaruh ke seluruh jaringan.

Metode yang digunakan dalam mengirim data dalam ring dinamakan "token passing". Token ini dikirim dari komputer satu ke yang lain sampai ke komputer yang dituju. Komputer yang mengirimkan token akan memodifikasi token tersebut, menambahkan alamat pada data dan mengirimkannya. Komputer yang dituju atau yang menerima akan mengirimkan pesan bahwa data telah diterima setelah diverifikasi dengan membuat token baru dan dikirim ke jaringan.

Terlihat proses pengiriman token ini akan memakan waktu yang lama, sebenarnya tidak, karena token ini bekerja dengan kecepatan cahaya. Sebuah token dapat berkeliling lingkaran (ring) sejauh 200 meter sebanyak 10,000 kali dalam satu detik.



Jenis kabel yang digunakan pada topologi ini adalah kabel coaxial. Perangkat jaringan dihubungkan dengan menggunakan TEE connector. Kesulitan utama dari penggunaan kabel coaxial ini adalah sulit untuk mengukur kabel coaxial agar cocok. Kalau tidak diukur dengan benar maka akibatnya dapat merusak NIC yang dipergunakan dan kinerja jaringan menjadi terhambat, tidak optimal. Topologi ini juga bisa menggunakan kabel fiber optic

Kelebihan :

- Mudah untuk menambahkan komputer atau peralatan lain ke jaringan
- Memerlukan kabel yang lebih sedikit dibandingkan dengan topologi star

Kekurangan :

- Seluruh jaringan akan tidak dapat berjalan jika ada kerusakan pada kabel utama
- Terminator diperlukan pada kedua ujung dari kabel backbone

Peraturan untuk pemasangan kabel :

1. Hindarilah pemasangan kabel jaringan yang sejajar (atau berdekatan) dengan kabel listrik.
2. Hindarilah pembengkokan kabel secara berlebih dan untuk penggulungan kabel memiliki diameter minimal 30cm
3. Jika akan melakukan penggabungan kabel menggunakan kabel pengikat, janganlah mengikat terlalu kencang sehingga menyebabkan deformasi pada kabel
4. Jauhkan kabel dengan perangkat yang dapat menyebabkan noise semisal mesin fotokopi, pemanas air, speaker, microwave, telepon, dll.
5. Hindarilah menarik kabel dengan terlalu kencang
6. Hindarilah pemasangan kabel UTP pada luar gedung karena rentan terhadap sambaran petir.

Sebelum melakukan instalasi atau pemasangan kabel, dilakukan pemeriksaan terhadap kabel yang akan dipasang. Pemeriksaan ini dilakukan baik untuk kabel coaxial maupun kabel UTP. Hal ini bertujuan untuk mengetahui kabel yang tidak dapat digunakan (mis: karena isinya terputus). Setelah kabel dipasang, gunakan pipa penutup agar rapi (ducking). Pemberian tanda pada kabel sebaiknya diterapkan agar memudahkan pengawasan ataupun perbaikan jika terjadi suatu kerusakan.

Dapat diketahui bahwa sistem pengkabelan di Indonesia belum terdesain dengan baik, hal ini terbukti karena kabel-kabel jaringan yang terinstal tidak berada dalam suatu dinding atau tembok dan berkeliaran bebas hingga dapat mengganggu aktivitas harian.

Untuk memasang kabel, harus berangkat dari ruangan server. Dengan kata lain, semua ujung kabel diratakan di ruangan server dekat dengan Hub. Misalkan memasang dan menarik kabel untuk 20 unit PC dan sisanya untuk server dan workstation di ruangan server. Tarik satu per satu kabel dan sesuaikan dengan keinginan, dengan perincian sebagai berikut:

- Panjang kabel UTP dari Hub ke Server maksimal 8 meter
- Panjang kabel UTP dari Hub ke Workstation di ruangan server maksimal 12 meter
- Panjang kabel UTP dari Hub ke Workstation di ruangan lainnya maksimal 100 meter.

2.5 Memasang Konektor Pada Kabel Jaringan

Pemasangan Konektor pada kabel UTP

Seseorang yang ingin memasang konektor harus mengetahui susunan kabel yang akan dipasang. Asal sama ujung ke ujung bisa saja, akan tetapi cara ini tidak tepat. Harus diperhatikan warna-warnanya. Untuk lebih jelasnya ikuti langkah-langkah berikut ini:

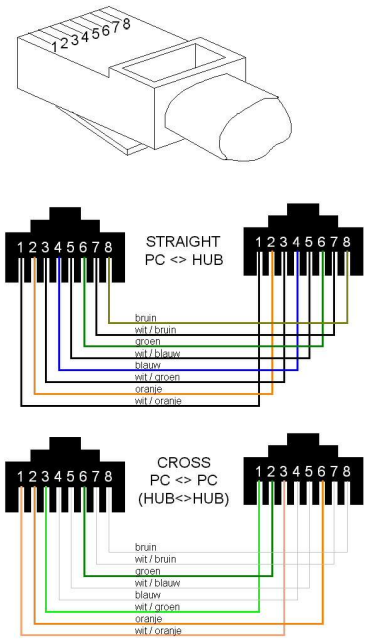
- Potong kabel UTP dengan menggunakan tang pemotong disesuaikan dengan panjang yang dibutuhkan untuk menyambungkan dua buah peralatan yang akan disambungkan (komputer dengan switch atau switch dengan switch, dll) serta disesuaikan pula dengan ketentuan yang berlaku mengenai panjang kabel maksimal (lihat catatan di atas)
- Kupas bagian luar dari kedua ujung kabel UTP tersebut sepanjang kurang lebih 2 cm.
- Lepasakan pilinan yang ada pada setiap pasang kabel tersebut dan luruskan masing-masing kabel tersebut hingga mudah untuk disusun
- Susun urutan warna sesuai dengan ketentuan berikut (untuk keterangan mengenai penggunaan straight atau throught silahkan melihat catatan pada bagian awal modul ini).

- Untuk kabel straight through, maka posisi warnanya untuk satu konektor ke konektor lain ditampilkan pada tabel berikut.

Putih Orange		Putih Orange
Orange		Orange
Putih Hijau		Putih Hijau
Biru		Biru
Putih Biru		Putih Biru
Hijau		Hijau
Putih Coklat		Putih Coklat
Coklat		Coklat

- Untuk kabel cross, maka posisi warnanya untuk satu konektor ke konektor lain ditampilkan pada tabel berikut.

Putih Orange		Putih Hijau
Orange		Hijau
Putih Hijau		Putih Orange
Biru		Biru
Putih Biru		Putih Biru
Hijau		Orange
Putih Coklat		Putih Coklat
Coklat		Coklat



- Siapkan konektor RJ-45 dan masukkan kabel. Setiap ujung konektor posisinya harus sama. Selain itu, bagian luar atau pembungkus kabel harus tejenpit agar kokoh dan tidak goyang.
- Setelah kabel masuk dan rata sampai ujung konektor, masukkan konektor dan jepit dengan tang crimping.
- Lakukan dengan hati-hati agar tidak ada konektor yang berpindah pada pin yang lain.

Lakukan hal yang sama untuk ujung kabel. Ingat ketentuan warnanya

Pemasangan Konektor pada kabel coaxial

1. Kuliti kabel coaxial dengan penampang melintang pada kedua ujung kabel sepanjang kurang lebih 4 cm.
2. Jangan sampai terjadi goresan berlebihan karena perambatan gelombang mikro adalah pada permukaan kabel
3. Pasang konektor dengan cermat dan memperhatikan penuh masalah kerapian
4. Solder pin ujung konektor dengan cermat dan rapi, pastikan tidak terjadi hubungan pendek (short) pada ujung konektor tersebut.

5. Perhatikan urutan pemasangan pin dan kuncian sehingga dudukan kabel dan konektor tidak mudah bergeser. Test kemungkinan terjadinya arus pendek (short) dengan multimeter
6. Tutup permukaan konektor dengan aluminium foil untuk mencegah kebocoran dan interferensi, posisi harus menempel pada permukaan konektor
7. Lapisi konektor dengan aluminium foil dan lapisi seluruh permukaan sambungan konektor dengan isolator TBA (biasa untuk pemasangan pipa saluran air atau kabel listrik instalasi rumah), atau isolasi 3 M. Lapisi juga dengan silicon gel
8. Tutup seluruh permukaan dengan isolator karet bakar untuk mencegah air
9. Untuk perawatan, ganti semua lapisan pelindung setiap 6 bulan sekali
10. Konektor terbaik adalah model hexa (crimp) tanpa solderan dan drat (screw) sehingga sedikit melukai permukaan kabel, yang dipasang dengan crimping tools, disertai karet bakar sebagai pelindung pengganti isolator karet.

3. Menguji konektivitas kabel

Pengujian konektivitas kabel UTP

Setelah pemasangan konektor RJ-45 pada kabel UTP telah selesai dilakukan maka hendaknya dilakukan pengujian atas kabel tersebut. Pengujian tersebut dilakukan bertujuan untuk mengecek mengenai konektivitas pada setiap pasang kabel tersebut serta untuk menghindari terjadi kesalahan pemasangan kabel pada posisi pin yang salah. Langkah-langkah yang harus dilakukan untuk melakukan pengecekan konektivitas kabel tersebut adalah :

1. Siapkan perangkat network tester (untuk keterangan lebih detail mengenai network tester silahkan lihat pada bagian atas modul ini)

Network Tester

2. Siapkan kabel yang akan dilakukan pengetesan
3. Hubungkan kedua ujung kabel tersebut pada konektor yang terdapat pada masing-masing port kabel tester.
4. Nyalakan network tester dan perhatikan pada lampu yang menyala, apakah lampu yang menyala sudah sesuai dengan pasangan konektivitas kabel (straight through ataupun crossover)
5. Jika ada lampu yang seharusnya menyala tetapi tidak menyala atau jika ada pasangan lampu yang salah nyalanya, berarti kabel yang telah dibuat tersebut salah dan harus diulang lagi pembuatannya yaitu dengan cara mengulangi kembali langkah-langkah pemasangan konektor UTP seperti yang dituliskan pada bagian atas modul ini.

Pengujian konektivitas kabel coaxial

Setelah pemasangan konektor BNC pada kabel coaxial telah selesai dilakukan maka hendaknya dilakukan pengujian atas kabel tersebut. Pengujian tersebut dilakukan bertujuan untuk mengecek mengenai konektivitas pada kabel coaxial tersebut apakah telah tersambung dengan optimal. Langkah-langkah yang harus dilakukan untuk melakukan pengecekan konektivitas kabel tersebut adalah :

1. Siapkan perangkat network tester (untuk keterangan lebih detail mengenai network tester silahkan lihat pada bagian atas modul ini)

Network Tester

2. Siapkan kabel yang akan dilakukan pengetesan

3. Hubungkan kedua ujung kabel tersebut pada konektor yang terdapat pada masing-masing port kabel tester.
4. Nyalakan network tester dan perhatikan pada lampu yang menyala, apakah lampu yang menyala sudah sesuai dengan pasangan konektivitas kabel
5. Jika lampu yang seharusnya menyala tetapi tidak menyala, berarti kabel yang telah dibuat tersebut salah dan harus diulang lagi pembuatannya yaitu dengan cara membuka konektor tersebut dan mencari kemungkinan mengenai adanya pemasangan antara konektor dengan kabel yang kendor atau mengulangi kembali langkah-langkah pemasangan konektor UTP seperti yang dituliskan pada bagian atas modul ini.

BAB 3
Memasang Jaringan Nirkabel

3.1 Pengenalan jaringan

Jaringan / *network* adalah suatu mekanisme yang memungkinkan berbagai komputer terhubung dan para penggunanya dapat berkomunikasi dan *share resources* satu sama. Informasi dan data bergerak melalui media transmisi jaringan sehingga memungkinkan pengguna jaringan komputer untuk saling bertukar dokumen dan data, mencetak pada *printer* yang sama dan bersama-sama menggunakan *hardware* / *software* yang terhubung dengan jaringan.

Saat ini kita mengenal beberapa jenis jaringan pada umumnya yatu jaringan data dan internet.

Jaringan data adalah sebuah jaringan yang memungkinkan komputer-komputer yang ada saling bertukar data. Contoh yang paling sederhana adalah dari jaringan data adalah dua buah PC terhubung melalui sebuah kabel. Akan tetapi rata-rata jaringan data menghubungkan banyak alat.

Jaringan internet adalah sekumpulan jaringan-jaringan yang saling terhubung oleh alat jaringan dan akan menjadikan jaringan-jaringan tersebut sebagai satu jaringan yang besar. Public Internet adalah contoh yang paling mudah dikenali sebagai jaringan tunggal yang menghubungkan jutaan komputer.

3.2 Arsitektur Jaringan

Ada 3 jenis arsitektur jaringan data.

1. LAN (*Local Area Network*)

Jaringan ini beroperasi dalam area yang jaraknya terbatas(kurang dari 10 kilometer).Biasanya jaringan ini bersifat tertutup karena hanya digunakan oleh sekumpulan orang dan memberikan akses bandwith yang tinggi dalam lingkup kelompok yang menggunakannya.Alat yang biasa digunakan adalah Switch dan Hub.

2. WAN (*Wide Area Network*)

Jaringan ini beroperasi dalam area yang lebih luas dari LAN.Biasanya jaringan WAN berfungsi untuk menghubungkan LAN yang berada terpisah secara geografis. Biasanya digunakan juga untuk fulltime/partime connectivity antar daerah dan juga untuk public services seperti email. Alat yang biasa digunakan di jaringan ini adalah Router.

3. MAN (*Metropolitan Area Network*)

Jaringan ini beroperasi dalam area yang lebih luas secara geografis.Biasanya menghubungkan jaringan WAN yang terpisah sehingga memungkinkan untuk terjadinya pertukaran informasi dan sharing data dan devices. Alat yang digunakan adala kumpulan dari Router dan Gateway.

Jaringan nirkabel adalah jaringan yang memungkinkan setiap user untuk saling bertukar informasi tanpa harus terhubung dengan kabel pada umumnya(UTP) sehingga memudahkan user untuk berpindah-pindah lokasi selama jaringan nirkabel tersebut dapat terhubung.

3.3 Tipe dari Jaringan Nirkabel

Sama halnya seperti jaringan yang berbasis kabel, maka jaringan nirkabel dapat diklasifikasikan ke dalam beberapa tipe yang berbeda berdasarkan pada jarak dimana data dapat ditransmisikan.

*** Wireless Wide Area Networks (WWANs)**

Teknologi WWAN memungkinkan pengguna untuk membangun koneksi nirkabel melalui jaringan publik maupun privat. Koneksi ini dapat dibuat mencakup suatu daerah yang sangat luas, seperti kota atau negara, melalui penggunaan beberapa antena atau juga sistem satelit yang diselenggarakan oleh penyelenggara jasa telekomunikasinya. Teknologi WWAN saat ini dikenal dengan sistem 2G (second generation). Inti dari sistem 2G ini termasuk di dalamnya Global System for Mobile Communications (GSM), Cellular Digital Packet Data (CDPD) dan juga Code Division Multiple Access (CDMA). Berbagai usaha sedang dilakukan untuk transisi dari 2G ke teknologi 3G (third generation) yang akan segera menjadi standar global dan memiliki fitur roaming yang global juga. ITU juga secara aktif dalam mempromosikan pembuatan standar global bagi teknologi 3G.

*** Wireless Metropolitan Area Networks (WMANs)**

Teknologi WMAN memungkinkan pengguna untuk membuat koneksi nirkabel antara beberapa lokasi di dalam suatu area metropolitan (contohnya, antara gedung yang berbeda-beda dalam suatu kota atau pada kampus universitas), dan ini bisa dicapai tanpa biaya fiber optic atau kabel tembaga yang terkadang sangat mahal. Sebagai tambahan, WMAN dapat bertindak sebagai backup bagi jaringan yang berbasis kabel dan dia akan aktif ketika jaringan yang berbasis kabel tadi mengalami gangguan. WMAN menggunakan gelombang radio atau cahaya infrared untuk mentransmisikan data. Jaringan akses nirkabel broadband, yang memberikan pengguna dengan akses berkecepatan tinggi, merupakan hal yang banyak diminati saat ini. Meskipun ada beberapa teknologi yang berbeda, seperti multichannel multipoint distribution service (MMDS) dan local multipoint distribution services (LMDS) digunakan saat ini, tetapi kelompok kerja IEEE 802.16 untuk standar akses nirkabel broadband masih terus membuat spesifikasi bagi teknologi-teknologi tersebut.

*** Wireless Local Area Networks (WLANs)**

Teknologi WLAN membolehkan pengguna untuk membangun jaringan nirkabel dalam suatu area yang sifatnya lokal (contohnya, dalam lingkungan gedung kantor, gedung kampus atau pada area publik, seperti bandara atau kafe). WLAN dapat digunakan pada kantor sementara atau yang mana instalasi kabel permanen tidak diperbolehkan. Atau WLAN terkadang dibangun sebagai suplemen bagi LAN yang sudah ada, sehingga pengguna dapat bekerja pada berbagai lokasi yang berbeda dalam lingkungan gedung. WLAN dapat dioperasikan dengan dua cara. Dalam infrastruktur WLAN, stasiun wireless (peranti dengan network card radio atau eksternal modem) terhubung ke access point nirkabel yang berfungsi sebagai bridge antara stasiun-stasiun dan network backbone yang ada saat itu. Dalam lingkungan WLAN yang sifatnya peer-to-peer (ad hoc), beberapa pengguna dalam area yang terbatas, seperti ruang rapat, dapat membentuk suatu jaringan sementara tanpa menggunakan access point, jika mereka tidak memerlukan akses ke sumber daya jaringan.Pada tahun 1997, IEEE meng-approve standar 802.11 untuk WLAN, yang mana menspesifikasikan suatu data transfer rate 1 sampai 2 megabits per second (Mbps). Di bawah 802.11b, yang mana menjadi standar baru yang dominan saat ini, data ditransfer pada kecepatan maksimum 11 Mbps melalui frekuensi 2.4 gigahertz (GHz). Standar yang lebih baru lainnya adalah 802.11a, yang mana menspesifikasikan data transfer pada kecepatan maksimum 54 Mbps melalui frekuensi 5 GHz.

*** Wireless Personal Area Networks (WPANs)**

Teknologi WPAN membolehkan pengguna untuk membangun suatu jaringan nirkabel (ad hoc) bagi peranti sederhana, seperti PDA, telepon seluler atau laptop. Ini bisa digunakan dalam ruang operasi personal (personal operating space atau POS). Sebuah POS adalah suatu ruang yang ada disekitar orang, dan bisa mencapai jarak sekitar 10 meter. Saat ini, dua teknologi kunci dari WPAN ini adalah Bluetooth dan cahaya infra merah. Bluetooth merupakan teknologi pengganti kabel yang menggunakan gelombang radio untuk mentransmisikan data sampai dengan jarak sekitar 30 feet. Data Bluetooth dapat ditransmisikan melewati tembok, saku ataupun tas. Teknologi Bluetooth ini digerakkan oleh suatu badan yang bernama Bluetooth Special Interest Group (SIG), yang mana mempublikasikan spesifikasi Bluetooth versi 1.0 pada tahun 1999. Cara alternatif lainnya, untuk menghubungkan peranti dalam jarak sangat dekat (1 meter atau kurang), maka user bisa menggunakan cahaya infra merah.Untuk menstandarisasi pembangunan dari teknologi WPAN, IEEE telah membangun kelompok kerja 802.15 bagi WPAN. Kelompok kerja ini membuat standar WPAN, yang berbasis pada spesifikasi Bluetooth versi 1.0. Tujuan utama dari standarisasi ini adalah untuk mengurangi kompleksitas, konsumsi daya yang rendah, interoperabilitas dan bisa hidup berdampingan dengan jaringan 802.11.

Jaringan Komputer Nirkabel memberikan fleksibilitas dalam instalasi dan konfigurasi dan kebebasan berhubungan dengan mobilitas jaringan, berikut adalah hal yang harus dipertimbangkan dalam menjalankan sistem Jaringan Komputer Nirkabel :

1. Jangkauan dan Liputan

Jangkauan komunikasi Radio Frequency (RF) dan Infrared (IR) merupakan sebuah fungsi dari desain produk (termasuk kekuatan transmit dan desain receiver) dan bentuk perambatan, terutama dalam lingkungan ruang tertutup. Interaksi terhadap objek bangunan, termasuk tembok, logam dan bahkan manusia, dapat mempengaruhi energi perambatan, untuk itulah pertimbangan jangkauan dan liputan perlu dipertimbangkan.

Benda-benda padat menghentikan signal infrared, yang mengakibatkan keterbatasan. Kebanyakan sistem Jaringan Komputer Nirkabel menggunakan Radio Frequency (RF) karena gelombang radio dapat melewati beberapa jenis ruangan dan hambatan lain.

Jangkauan (atau radius liputan) untuk sistem Jaringan Komputer Nirkabel tipikal bervariasi mulai dari di bawah 100 kaki sampai lebih dari 300 kaki. Jangkauan dapat diperluas, dan kebebasan bergerak via roaming, dapat dilakukan menggunakan microcells.

2. Throughput

Seperti halnya dengan sistem Jaringan Komputer Berkabel , throughput yang sebenarnya dalam Jaringan Komputer Nirkabel tergantung pada produk dan jenis set-up. Faktor-faktor yang mempengaruhi throughput termasuk jumlah pengguna, faktor-faktor yang mempengaruhi perambatan misalnya jarak dan multipath, tipe Jaringan Komputer Nirkabel yang digunakan, seperti latency dan bottleneck pada bagian Jaringan Komputer Berkabel.

Rate data untuk kebanyakan Jaringan Komputer Nirkabel komersial adalah sekitar 1.6Mbps. Para pengguna topologi Ethernet tradisional atau Token Ring biasanya merasakan sedikit perbedaan ketika menggunakan Jaringan Komputer Nirkabel.

Jaringan Komputer Nirkabel menyediakan throughput yang cukup untuk kebanyakan aplikasi Jaringan Komputer kantoran, termasuk pertukaran electronic mail (E-Mail), akses ke peralatan bersama mis printer, akses internet, dan akses untuk database dan aplikasi multi-user. Sebagai perbandingan, jika sebuah modem terbaru dengan teknologi V.90 mengirim dan menerima data pada data rate 56.6 Kbps, maka dalam hal throughput sebuah Jaringan Komputer Nirkabel beroperasi pada 1.6Mbps artinya hampir tigapuluh kali lebih cepat.

3. Integritas dan Reliabilitas

Teknologi nirkabel telah diuji selama lebih dari limapuluh tahun dalam aplikasi nirkabel di dunia komersial dan militer. Walaupun interferensi radio dapat mengakibatkan degradasi dalam hal throughput, gangguan semacam itu sangat jarang terjadi dalam ruang kantor.

Desain yang bagus dari produsen alat teknologi Jaringan Komputer Nirkabel yang telah terbukti dan aturan batas jarak signal menghasilkan koneksi yang lebih bagus daripada koneksi telpon selular dan memberikan integritas data yang performanya sama atau bahkan lebih bagus daripada Jaringan Berkabel.

4. Kompatibilitas dengan Jaringan yang Telah Ada

Kebanyakan Jaringan Komputer Nirkabel telah disiapkan untuk memenuhi standar industri interkoneksi dengan Jaringan Berkabel seperti Ethernet atau Token Ring serta didukung oleh sistem operasi jaringan sama halnya dengan Jaringan Komputer Berkabel melalui penggunaan driver yang tepat. Setelah terinstal, maka jaringan akan menganggap komputer nirkabel sama seperti komponen jaringan yang lain.

5. Interoperabilitas Perangkat Jaringan Nirkabel

Calon pengguna harus menyadari bahwa perangkat sistem Jaringan Komputer Nirkabel dari beberapa produsen mungkin tidak saling interoperable (tidak kompatibel), untuk tiga alasan berikut ini .

Pertama, teknologi yang berbeda tidak saling mendukung. Sebuah sistem yang berbasis teknologi spread spectrum frequency hopping (FHSS) tidak akan berkomunikasi dengan sistem lain yang berbasis teknologi spread spectrum direct sequence (DSSS).

Kedua, sistem yang menggunakan band frekuensi yang berbeda tidak akan saling berkomunikasi walaupun keduanya menggunakan teknologi yang sama. Ketiga, sistem dari produsen yang berbeda kemungkinan tidak akan berhubungan walaupun keduanya menggunakan teknologi yang sama dan band frekwensi yang sama, sehubungan dengan perbedaan implementasi (teknologi) pada setiap produsen.

6. Interferensi dan Ko-eksistensi

Dengan tidak adanya aturan lisensi frekwensi pada produk-produk perangkat Jaringan Komputer Nirkabel, berarti produk lain yang memancarkan energi dalam spektrum frekwensi yang sama secara potensial dapat mengakibatkan interferensi terhadap sistem komputer nirkabel. Sebagai contoh adalah oven microwave, tapi sebagian besar produsen perangkat Jaringan Komputer Nirkabel telah mendesain produk mereka dengan memperhitungkan interferensi oven microwave.

Hal lain yang patut dipertimbangkan adalah penggunaan beberapa merek perangkat Jaringan Komputer Nirkabel dari produsen yang berbeda-beda. Sementara produk dari beberapa produsen menginterferensi merek lain, beberapa produk tidak saling interferensi.

7. Izin Penggunaan Frekuensi

Di Amerika Serikat, Federal Communications Commissions (FCC) mengatur penggunaan transmisi radio, termasuk yang digunakan dalam Jaringan Komputer Nirkabel. Negara lain juga memiliki lembaga yang mengatur hal tersebut.

Perangkat Jaringan Komputer Nirkabel secara tipikal didesain untuk beroperasi pada bagian spektrum radio di mana FCC tidak mensyaratkan end-user untuk membayar izin penggunaan gelombang radio. Di Amerika Serikat, umumnya Jaringan Komputer Nirkabel menggunakan frekwensi pada salah satu gelombang ISM (Instrumentation, Scientific, and Medical). Ini termasuk 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, dan 5.725-5.875 GHz.

Agar dapat menjual perangkat Jaringan Komputer Nirkabel di suatu negara, produsen harus memperoleh sertifikasi dari lembaga terkait dinegara yang dimaksud.

8. Kemudahan dalam Penggunaan

Pengguna hanya perlu mendapat sedikit informasi baru untuk dapat segera menggunakan Jaringan Komputer Nirkabel. Karena tipikal Jaringan Komputer Nirkabel yang kompatibel dengan Network Operating System, maka aplikasi-aplikasi akan berfungsi sama dengan ketika menggunakan Jaringan Komputer Berkabel.

Selain itu sistem Jaringan Komputer Nirkabel juga menggabungkan beberapa alat diagnostik untuk mengetahui masalah yang mungkin timbul dengan elemen-elemen sistem nirkabel; namun bagaimanapun juga, sistem telah dirancang agar kebanyakan pengguna tidak perlu sampai menggunakan alat diagnostik tersebut.

Jaringan Komputer Nirkabel menyederhanakan banyak aturan-aturan dalam hal instalasi dan konfigurasi yang memusingkan para manajer jaringan. Karena hanya Titik Akses (transceiver) yang membutuhkan kabel, maka para manajer jaringan dibebaskan dari urusan menarik kabel.

Dengan sedikitnya kabel yang digunakan maka sangat mudah untuk memindahkan, menambah dan mengubah konfigurasi dalam jaringan. Terakhir, sifat portable (mudah dipindahkan) dari Jaringan Komputer Nirkabel, memberikan keleluasaan bagi manajer jaringan untuk melakukan pra-konfigurasi dan memperbaiki seluruh jaringan sebelum memasang pada lokasi yang terpisah.

Setelah terkonfigurasi, Jaringan Komputer Nirkabel dapat dipindahkan ke tempat lain hanya dengan sedikit modifikasi atau tanpa modifikasi sama sekali.

9. Keamanan

Karena teknologi nirkabel berasal dari aplikasi militer, maka faktor keamanan sejak lama merupakan kriteria terutama dalam perangkat nirkabel. Standar keamanan secara tipikal merupakan bagian daripada Jaringan Komputer Nirkabel, membuatnya menjadi lebih aman daripada kebanyakan Jaringan Komputer Berkabel.

Sangat sulit bagi orang luar untuk menyadap lalulintas Jaringan Komputer Nirkabel. Teknik enksripsi yang kompleks membuat hal tersebut sangat sulit dimungkinkan, sehingga yang perlu diawasi adalah penggunaan akses ke jaringan.

Secara umum, sebuah klien harus dibuat seaman mungkin sebelum diizinkan ikut serta dalam sebuah Jaringan Komputer Nirkabel.

10. Biaya

Implementasi sebuah Jaringan Komputer Nirkabel melibatkan biaya infrastruktur pada titik-titik akses nirkabel dan biaya pengguna untuk setiap kartu adapter nirkabel.

Biaya infrastruktur utamanya tergantung pada jumlah Titik Akses yang dipasang; harga sebuah Titi k Akses berkisar US$ 1,000 sampai $ 2,000. Jumlah Titik Akses secara tipikal tergantung pada wilayah jangkauan yang ingin diliput dan atau jumlah atau tipe pengguna yang ingin dilayani. Wilayah liputan proporsional dengan jangkauan produk. Kartu adapter Jaringan Komputer Nirkabel dibutuhkan untuk platform standar komputer, harganya berkisar US$ 300 sampai dengan US$ 1,000.

Biaya pemasangan dan pemeliharaan sebuah Jaringan Komputer Nirkabel umumnya lebih murah daripada biaya pemasangan dan pemeliharaan Jaringan Komputer Berkabel, dengan dua alasan.

Pertama, sebuah Jaringan Komputer Nirkabel menghilangkan biaya kabel dan ongkos kerja memasang dan memperbaikinya. Kedua, karena Jaringan Komputer

Nirkabel memudahkan pemindahan, penambahan dan perubahan, maka mengurangi biaya tidak langsung user-downtime dan biaya overhead administratif.

11. Skalabilitas

Jaringan Komputer Nirkabel dapat dirancang menjadi sangat mudah atau sangat rumit. Jaringan Komputer Nirkabel dapat mendukung banyak klien dan atau wilayah liputan dengan menambah Titik Akses (transceiver) untuk memperkuat atau memperluas liputan.

12. Pengaruh Terhadap Kesehatan

Radiasi yang dihasilkan dari Jaringan Komputer Nirkabel sangat rendah, lebih kecil daripada yang dihasilkan telepon selular. Karena gelombang radio memudar dengan cepat, maka radiasi yang terkirim hanya sebagian kecil yang menerpa orang-orang yang bekerja dalam sistem Jaringan Komputer Nirkabel.

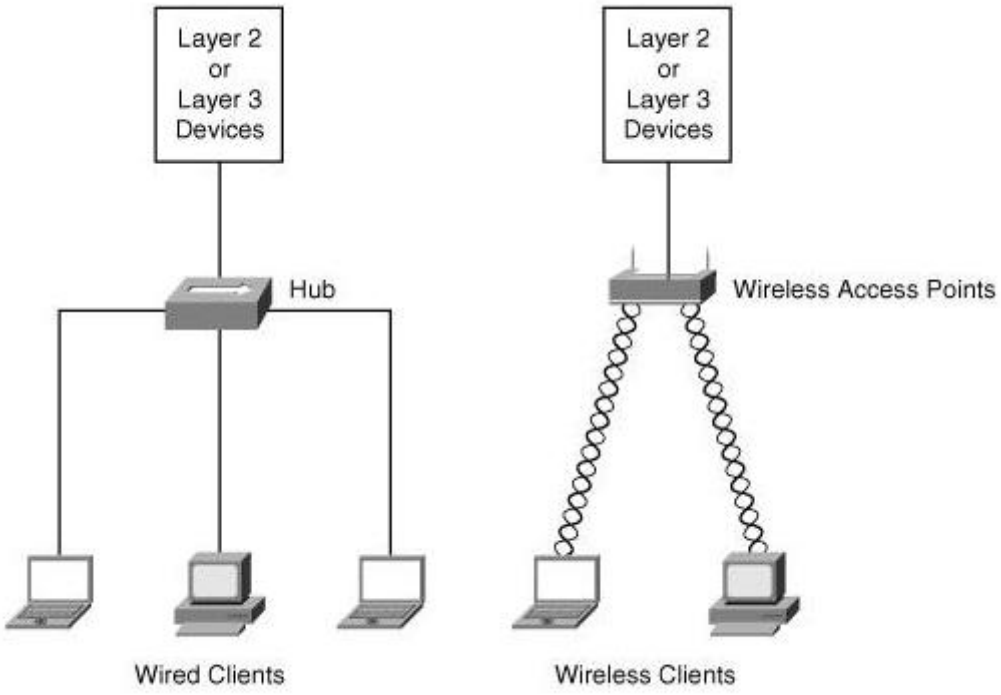
Kesimpulan

Fleksibilitas dan mobilitas membuat Jaringan Komputer Nirkabel sebagai pelengkap yang efektif dan alternatif menarik dibandingkan Jaringan Komputer Berkabel. Jaringan Komputer Nirkabel menyediakan semua fungsi yang dimiliki oleh Jaringan Komputer Berkabel, tanpa perlu terhubung secara fisik.

Konfigurasi Jaringan Komputer Nirkabel mulai dari topologi yang sederhana peer-to-peer sampai dengan jaringan yang kompleks menawarkan konektivitas distribusi data dan roaming. Selain menawarkan mobilitas untuk pengguna dalam lingkungan yang dicakup oleh jaringan, juga memungkinkan jaringan portable, memungkinkan jaringan untuk berpindah dengan pengetahuan penggunanya.

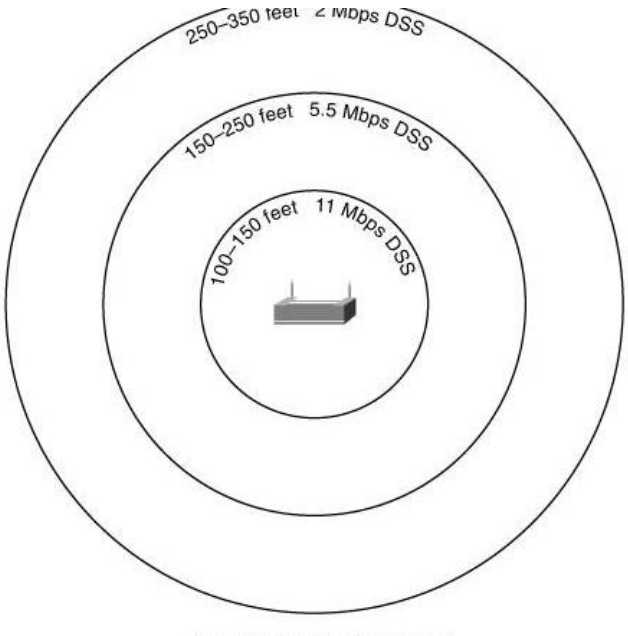
1. Sekilas Teknologi Nirkabel

Dalam bentuk yang paling sederhana ,jaringan nirkabel adalah LAN yang menggunakan frekuensi radio untukdapat salaing berkomunikasi ketimbang menggunakan kabel.Contoh gambar di bawah menunjukan klien device berhubungan dengan access point.



Gambar 1. Jaringan Kabel dan Jaringan Nirkabel

Karena jaringan Nirkabel menggunakan frekuensi radio ,maka kecepatan akses tergantung pada jarak antara transmiter dan receiver.Maka semakin dekat klien device dengan access point semakin besar kecepatan akses mereka dalam jaringan .



Gambar 2. Akses data dipengaruhi jarak akses ke transmiter frekuensi radio

3.4 Komponen Jaringan Nirkabel

Berikut adalah komponen Jaringan Nirkabel :

1.Access point

2. Klien Device

3.Switch

4.Kabel

1. Access Point

Access Point menyediakan konektifitas antara device-device dengan jaringan nirkabel yang ada. Access point terbagi menjadi 2 yaitu :

a. Access Point

Access Point yang dimaksud di sini berfungsi sebagai media yang memberikan konektifitas antara klien device dengan jaringan yang ada.Biasanya antara access point dengan PDA atau Handphone yang sudah memiliki perangkat nirkabel.Atau bisa juga antara access point dengan laptop yang memiliki perangkat nirkabel.

Pemasangan access point bisa dilakukan pada ruangan tertutup maupun ruangan terbuka.Jaringan Nirkabel memiliki standar tersendiri yang telah ditentukan oleh IEEE(Institute of Electrical and Electronics Engineers)

Tabel 1. Standar dalam Nirkabel

Standard	Maximum Throughput (Mbps)	Frequency (GHz)	Compatibility	Ratified
802.11b	11	2.4		1999
802.11a	54	5		1999; Product availability 2001
802.11g	54	2.4	Backward-compatible with	2003

Tabel 1. Standar dalam Nirkabel				
Standard	**Maximum Throughput (Mbps)**	**Frequency (GHz)**	**Compatibility**	**Ratified**
			802.11b	

Standar 802.11a bekerja dalam 5 Ghz band yang membuat transmisi mudah terinteferensi dari microwave dan telephon nirkabel.Kekuatan standar 802.11b dan 802.11g beroperasi dalam 2.4 Ghz band terpengaruh secara negatif oleh air, besi dan dinding tipis.

Standar 802.11b dan 802.11g membagi 2.4 GHz band menjadi 14 channel.Channel 1,6,dan 11 tidak akan menyebabkan overlapping(interferensi) apabila dipasang bersamaan dalam suatu jairngan. Standar 802.11a lebih rendah interferensi nya akan tetapi memerlukan line of sight (pandangan bebas dari halangan).

Metode akses medium dari standar 802.11, disebut dengan Distribution Coordination Method, sama dengan mekanisme yang ada dalam Ethernet yaitu carrier sense multiple access collision detect (CSMA/CD).

Gambar 3 Access Point Indoor

Gambar 4 Access Point Outdoor

b. Bridge

Access Point yang digunakan sebagai bridge berfungsi sebagai media yang memberikan konektifitas antara access point lain dengan jaringan yang ada.Biasanya access point ini sama-sama digunakan sebagai bridge.Access point digunakan sebagai bridge apabila hendak mengkonekkan antara 2 gedung yang berjauhan dan tidak mungkin dilewati oleh media lain (kabel) untuk menghubungkannya. Koneksi ini biasa disebut sebagai koneksi peer to peer.

Untuk memasang bridge lokasi yang dipasang harus bebas dari halangan (line of sight) yaitu tidak terhalang gedung lain atau pemancar lain sehingga tidak bentrok dalam memancarkan sinyal.Pemasangan bridge juga harus disertai pemasangan antena.

Gambar 5 Bridge

Ada 2 jenis antena yaitu: omni directional dan bi-directional.Antena omni directional mempunyai radius melingkar dan bisa mencakup banyak user apalagi ditempatkan pada tempat yang bebas dari halangan(tembok,tiang,dll). Antena bi-directional mempunyai radius yang berbeda. Sinyal yang dipancarkan lebih bersifat menembak satu point.

Gambar 6 Antenna Omni directional

Gambar 7 Antenna Bi-directional

a) Point-to-Point Bridging

Tidak selalu mudah untuk menjalankan sebuah jaringan kabel antara 2 gedung untuk menggabungkan LAN yang ada menjadi satu broadcast domain.Apabila kedua gedung mempunyai jarak yang masuk dalam jangkauan dan berada dalam direct line of sight satu dengan yang lain, maka bridge bisa digunakan.

Dengan menggunakan dua access point untuk menciptakan satu logik port bridge. Dalam model ini access point didedikasikan sebagai point-to point bridge dan tidak berfungsi sebagai access point untuk klien device.

Gambar 8. Point-to-Point Bridging

1. Klien Device

Klien Device biasanya dilengkapi dengan WIC(Wireless Interface Card) atau PCMIA Card Adapter di mana alat inilah yang menghubungkan klien device dengan access point melalui radio frequency.Contoh dari klien device adalah :

a. PC user
b. Laptop
c. PDAs
d. Handphone with wireless adapter

Gambar 9 PCMIA Card Adapter

Gambar 10 Contoh PDA yang support jaringan nirkabel

Gambar 11 Contoh Handphone yang support Jaringan Nirkabel

2. Switch

Switch dikenal juga dengan istilah LAN switch merupakan perluasan dari bridge. Ada dua buah arsitektur switch, sebagai berikut:

i. Cut through

Kelebihan dari arsitektur switch ini terletak pada kecepatan, karena pada saat sebuah paket datang, switch hanya memperhatikan alamat tujuan sebelum diteruskan ke segmen tujuannya.

ii. Store and forward

Switch ini menerima dan menganalisa seluruh isi paket sebelum meneruskannya k etujuan dan untuknya memerlukan waktu.

Keuntungan menggunakan switch apabila bila switch tersebut merupakan base Ethernet adalah karena setiap segmen jaringan memiliki bandwith 10 Mbps penuh,dan 100 Mbps apabila base Fast Ethernet dan tidak terbagi seperti pada hub.

Gambar 12 Switch

4. Kabel

Kabel yang digunakan untuk jaringan nirkabel adalah sebagai berikut

1.1 Kabel UTP

Ada dua buah jenis kabel UTP yakni shielded dan unshielded. Shielded adalah kabel yang memiliki selubung pembungkus. Sedangkan unshielded tidak memiliki selubung pembungkus. Untuk koneksinya digunakan konektor RJ-45.

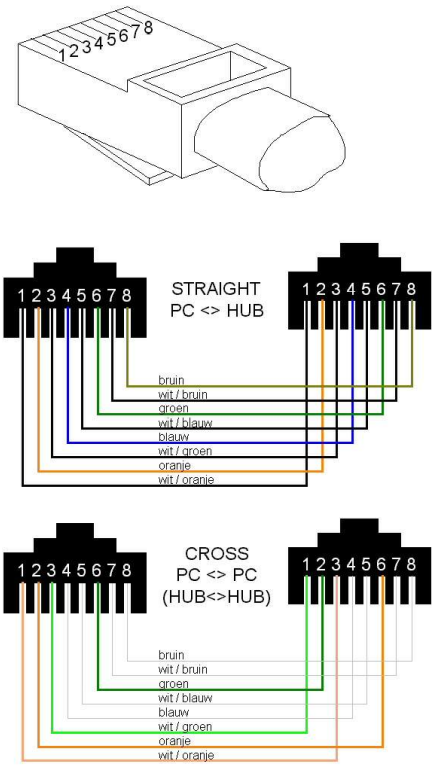
Gambar 13 Konektor RJ-45

UTP cocok untuk jaringan dengan skala dari kecil hingga besar. Dengan menggunakan UTP, jaringan disusun berdasarkan topologi star dengan hub sebagai pusatnya. Kabel ini umumnya lebih reliable dibandingkan dengan kabel koaksial.

Ada beberapa kategori dari kabel UTP. Yang paling baik adalah kategori 5. Ada dua jenis kabel, yakni straight-through dan crossed. Yang digunakan untuk koneksi dari access point ke switch adalah kabel Straight-through.

Untuk kabel kategori 5, ada 8 buah kabel kecil di dalamnya yang masing-masing memiliki kode warna. Akan tetapi hanya kabel 1,2,3,6. Walaupun demikian, ke delapan kabel tersebut semuanya terhubung dengan jack.

Untuk kabel straight-through, kabel 1, 2, 3, dan 6 pada suatu ujung juga di kabel 1,2,3, dan 6 pada ujung lainnya. Sedangkan untuk kabel crossed, ujung yang satu adalah kebalikan dari ujung yang lain (1 menjadi 3 dan 2 menjadi 6).



Gambar 14 Kabel UTP

1.2 Kabel koaksial

Media ini paling banyak digunakan sebagai media LAN, meski lebih mahal dan lebih sukar dibanding dengan UTP. Kabel ini memiliki bandwith yang lebar, oleh karena itu dapat digunakan untuk komunikasi broadband. Kabel jenis ini digunakan untuk menghubungkan access point dengan antena. Ada dua buah jenis kabel koaksial, sebagai berikut:

c. Thick Coaxial

Kabel jenis ini digunakan untuk kabel pada instalasi Ethernet antar gedung. Kabel ini dapat menjangkau jarak 500 m bahkan sampai 2500 m dengan memasang repeater.

d. Thin Coaxial

Kabel jenis ini cocok untuk jaringan rumah atau kantor. Kabel ini mirip seperti kabel antenna TV, harganya tidak mahal, dan mudah dipasangnya. Untuk memasangnya, kabel ini menggunakan konektor BNC.

3.5 Pengalamatan IP

1. IP Address

IP address adalah alamat logika yang diberikan ke peralatan jaringan yang menggunakan protokol TCP/IP. *IP address* terdiri dari 32 bit angka binari, yang ditulis dalam empat kelompok terdiri atas 8 bit (*oktat*) yang dipisah oleh tanda titik. Contohnya adalah : 11000000.00010000.00001010.00000001 atau dapat juga ditulis dalam bentuk empat kelompok angka desimal (0-255) misalnya 192.16.10.1. IP *address* yang terdiri atas 32 bit angka dikenal sebagai IP versi 4 (IPv4).

TCP/IP melihat semua IP *address* sebagai dua bagian jaringan, yaitu *network* ID dan *host* ID. *Network* ID menentukan alamat jaringan sedangkan *host* ID menentukan alamat *host* atau *komputer.* Oleh sebab itu, IP *address* memberikan alamat lengkap suatu komputer berupa gabungan alamat jaringan dan *host*. Jumlah kelompok angka yang termasuk *network* ID dan *host* ID tergantung pada kelas IP *address* yang dipakai.

2. Kelas-Kelas *IP Address*

IP *address* dapat dibedakan menjadi lima kelas, yaitu A, B, C, D, dan E (*Mansfield, 2002, p134*). Dalam hal ini kelas A, B, dan C digunakan untuk address biasa. Sedangkan kelas D digunakan untuk *multicasting* (224.0.0.0 – 239.255.255.255) dan kelas E (240.0.0.0 – 247.255.255.255) dicadangkan dan belum digunakan. Agar peralatan dapat mengetahui kelas suatu IP *address*, maka setiap IP harus memiliki *subnet mask*. Dengan memperhatikan default *subnet mask* yang diberikan, kelas suatu IP *address* dapat diketahui. Berikut pada tabel 2.1 dijelaskan mengenai pengelompokan kelas – kelas IP *address* beserta dengan jumlah jaringan dan jumlah *host* per jaringan yang dapat digunakan beserta *default subnet mask*-nya.

Tabel 2 Kelas – kelas IP *address*

Kelas IP *address*	**Kelompok oktat pertama**	***Network* ID**	***Host* ID**	**Jumlah jaringan**	**Jumlah host per jaringan**	***Default subnet mask***
A	1 – 126	w.	x.y.z	128	16.777.216	255.0.0.0
B	128 – 191	w.x	y.z	16.384	65.536	255.255.0.0
C	192 – 223	w.x.y	z	2.097.152	256	255.255.255.0

Dalam penggunaan IP address ada peraturan tambahan yang harus diketahui, yaitu :

- Angka 127 pada oktat pertama digunakan untuk *loopback*
- *Network* ID tidak boleh semuanya terdiri atas angka 0 atau 1
- *Host* ID tidak boleh semuanya terdiri atas angka 0 atau 1

Jika *host* ID berupa angka binari 0, IP *address* ini merupakan *network* ID jaringannya. Jika *host* ID semuanya berupa angkan binari 1, IP *address* ini biasanya digunakan untuk *broadcast* ke semua *host* dalam jaringan lokal.

3. Private IP address

Internet Assigned Number Authority (IANA) yang merupakan badan internasional, yang mengatur masalah pemberian IP *address* untuk digunakan dalam *internet*, menyediakan kelompok-kelompok IP *address* yang dapat dipakai tanpa pendaftaran yang disebut *private* IP *address*. *Private address* atau *non-routable* ini dialokasikan untuk digunakan pada jaringan yang tidak terkoneksi ke *internet*.

RFC 1918 bertemakan "*Address Allocation for Private Internets*" membahas tentang penggunaan jaringan / operasional jaringan menggunakan TCP/IP. Penggunaan IP publik dan *private* juga menjadi masalah yang dicermati berkenaan dengan *global address space* yang semakin berkurang setiap harinya. Berikut ini adalah set IP *private* yang direkomendasikan dalam RFC 1918.

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Gambar 15 Rekomendasi IP *private* dalam RFC 1918

2.6 Sekuritas Dasar Jaringan Nirkabel

Keamanan dasar nirkabel disediakan oleh hal-hal berikut :

- SSIDs(Service Set Identifiers)
- Wired Equivalent Privacy (WEP)
- Media Access Control (MAC) address verification

SSIDs

SSID merupakan suatu kode yang mengidentifikasikan hubungan dengan sebuah access point. Semua peralatan nirkabel yang hendak berkomunikasi dalam sebuah jaringan harus memiliki SSID yang sama parameternya karena SSID access point lah yang menciptakan konektifitas klien device dengan access point.

Secara standar, sebuah access point membroadcast SSIDnya setiap beberapa detik. Broadcase ini bisa dihentikan sehingga menyulitkan hacker untuk menemukan SSID dan kemudian mengambil alih kontrol dari access point. Akan tetapi, karena SSID termasuk dalam tanda dari setiap frame nirkabel,sangat mudah untuk hacker yang telah mempersiapkan untuk melakukan peralatan sniffing untuk menemukan parameter yang diset dan langsung terhubung dengan jaringan yang ada.

Apabila proses dapat bergabungnya dalam jaringan nirkabel dengan mengetahui SSID bisa disebut sebagai jaringan tersebut memiliki autentikasi terbuka

Wired Equivalent Privacy(WEP)

WEP bisa digunakan untuk mengatasi masalah broadacasr SSID dengan mengenkripsi trafik antara klien nirkabel dengan access point. Apabila terhubung ke dalam jaringan nirkabel menggunakan WEP bisa dikatakan jaringan tersebut melakukan autentikasi shared-key. Di mana access point melakukan challenge kepada klien nirkabel dan meminta klien untuk mengembalikan challenge tersebut secara terenkripsi. Apabila access point bisa mendekripsi respon dari klien makan klien tersebut terbukti mempunyai key yang valid dan mempunyai hal untuk terhubung dalam jaringan tersebut.

WEP ada dalam dua jenis panjang enkripsi : 64-bit dan128-bit.

Verifikasi MAC Address

Untuk keamanan nirkabel yang lebih lagi, seorang administrator jaringan bisa menggunakan filtering MAC address di mana access point dikonfigurasi untuk hanya menerima MAC address klien yang diperbolehkan untuk mengakses jaringan.Sayangnya metode ini juga kurang aman karena frame yang dikirim bisa saja disniff untuk mendapatkan MAC address.

Enhanced Wireless Security

Standar kemananan lebih kuat ditunjukan dalam tabel berikut dimana tujuan diciptakannya untuk menutupi kelemahan dalam WEP.

Table 3. Standar Keamanan Nirkabel

Komponen Keamanan	Standar 802.11 Awal	Peningkatan Keamanan
Authentication	Open authentication or shared-key	802.1x
Encryption	WEP	Wireless Fidelity (Wi-Fi) Protected Access (WPA), then 802.11i

802.1x

IEEE 802.1x adalah sebuah standar kontrol jaringan berdasarkan port.802.1x menyediakan per-user,per-session, mutual strong authentication, tidak hanya untuk jaringan nirkabel tapi juga untuk jaringan kabel bila diperlukan.

Berdasarkan ametode autentikasi yang digunakan, 802.1x juga menyediakan enkripsi.Berdasarkan IEEE Extensible Authorization Protocol (EAP), 802.1x memungkinkan access point dan klien untuk berbagi dan bertukar kunci enkripsi WEP secara otomatis. Access point akan bertindak sebagai proxy dan melakukan komputional dari enkripsi.Standar 802.1x juga mendukung manajemen kunci secara sentralisasi untuk Jaringan Nirkabel.

Wi-Fi Protected Access

WPA diperkenalkan sebagai solusi menengah untuk enkripsi WEP dan integritas data sementara IEEE 802.11i ditingkatkan.

Ketika WPA diimplementasikan , akses menuju WPA disediakan hanya untuk klien yang mempunyai hak. Walaupun WPA jauh lebih aman daripada WEP , preshared key disimpan dalam klien device sehingga apabila device klien ini dicuri, seorang hacker bisa dengan mudah mengakses jairngan nirkabel.

WPA mendukung autentikasi dan enkripsi.Autentikasi dilakukan dengan presharesd key yang diketahui sebagai WPA Personal,dan ketika dilakukan melalui 802.1x dikenal sebagai WPA Enterprise.

WPA menawarkan Temporal Key Integrity Protocol (TKIP) sebagai algoritma enkripsi dan sebuah algoritma yang terinttegrasi yan dikenal sebagai Michael.

802.11i

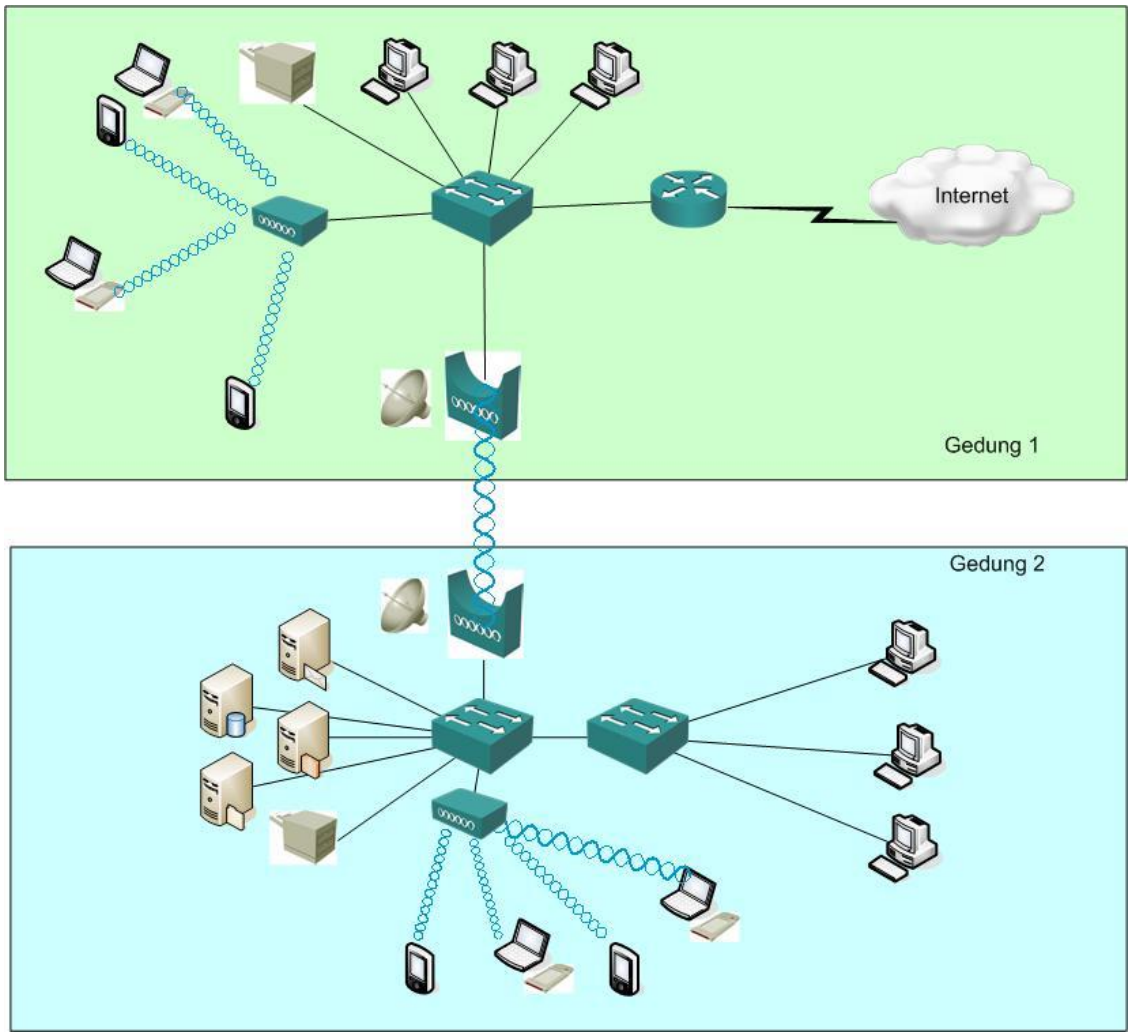
Standar 802.11i menggantikan WEP dan fitur keamanan lain ddari standar asal 802.11i .

WPA2 merupakan produk tersertifikasi yang dirancang untuk peralatan nirkabel yang kompatibel dengan standar 802.11i.Seritifikat WPA2 menyediakan support untuk fitur keamanan 802.11i yang tidak ada dalam WPA. WPA2 ,seperti WPA juga mendukung metode Enterprise dan Personal untuk autentikasi.

Sebagai tambahan untuk memperkuat kebutuhan enkripsi, WPA1 juga menambahkan peningkatan untuk fast roaming daripada klien device dengan mengijinkan klien untuk melakukan pre-autentikasi dengan access point ketika berpindah,sementara koneksi ke access point tetap terjaga walupun bergerak menjauh dari access point.

3.7 Perancangan Jaringan Nirkabel

3.7.1 Contoh Desain jaringan Nirkabel



Gambar 16 Desain Jaringan Nirkabel

Dari gambar di atas dapat dilihat bahwa ada sebuah perusahaan memiliki 2 gedung yang terpisah dan mereka menghubungkan jaringan kabel mereka dengan menggunakan access point bridge. Hal ini dapat saja disebabkan karena kondisi lapangan tidak memungkinkan untuk adanya penarikan kabel. Jadi koneksi yang dilakukan berupa peer to peer dengan menggunakan bridge untuk menghubungkan kedua gedung tersebut.

Di sini mereka menggunakan antena Bi-directional karena koneksinya hanya menunjuk pada satu arah saja.Sinyalnya tidak perlu menyebar.Untuk kemanannnya,SSID dari bridge sebaiknya dilakukan proses hidden(tidak dibroadcast/disebar sehingga hanya

access point atau *klien device* yang telah mengetahui SSID access point tersebut yang dapat mengakses).Perlu diingat bahwa kecepatan besar bandwith antar bride maksimum hanya dapat mencapai 54Mbps,akan tetapi kecepatan ini bisa menurun apabila ada hujan atau badai.

Dari gambar di atas juga bisa dilihat juga bahwa dalam gedung 1 dan 2 masing-masing memiliki access point untuk jaringan nirkabel.Di mana jaringan nirkabel ini bisa diakses baik oleh laptop yang telah memiliki perangkat nirkabel ataupun Handphone /PDA yang mendukung nirkabel. SSID untuk access point sebaiknya dilengkapi dengan keamanan tertentu seperti WEP atau WPA sehingga tidak sembarang user dapat mengakses jaringan dalam perusahaan tertentu.Untuk jumlah dan penempatan access point bisa disesuaikan dengan denah di perusahaan tersebut(bagaimana kondisi fisik dari gedung tersebut).

3.7.2 Hal-Hal yang harus diperhatikan dalam mendesain jaringan nirkabel

1. Site Survei

Site survei,awalnya jarang dilakukan karena biaya untuk implementasi jaringan nirkabel sangat murah sehingga tidak masalah berapa banyak access point yang hendak dipasang.Akan tetapi sangat disarankan untuk melakukan hal ini karena hal ini dapat membantu dalam memilih tempat untuk pemasangan access point selain masalah penyebaran sinyal hal ini bertujuan menghindari terjadinya tabrakan frekuensi.

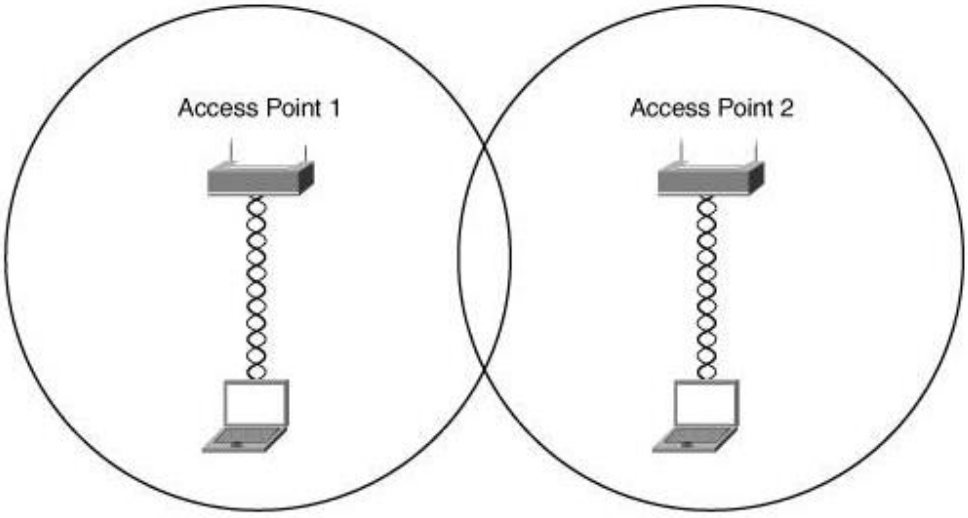
Ketika mengadakan site survei ,ada beberapa pertanyaan yang sebaiknya ditanyakan :

- Sistem nirkabel manakah yang mendukung aplikasi yang ada?
- Apakah kondisi line-of-sight sudah ada untuk antena?
- Di manakah access point sebaiknya diletakan supaya sedekat mungkin dengan klien yang akan mengakses access point.
- Apakah sumber potential interferensi yang ada dalam gedung tersebut?Mis: telepon nirkabel,microwave,interferensi alam,atau access point lain yang menggunakan channel frekuensi yang sama.

- Apakah ada pemerintahan,baik local atau propinsi dan legistatif yang harus dipertimbangkan dalam pemasangan access point?

2. Roaming Jaringan Nirkabel

Jaringan Nirkabel menghabiskan biaya yang lebih sedikit ketimbangan jaringan kabel ketika diimplementasikan. Besar kecepatan akses tergantung dari access point dan radius daerah jangkauan sebaiknya diperhitungkan dengan baik saat didesain karena apabila terjadi tabrakan channel frekuensi dengan acces point lain maka akan terjadi dead spots.Di mana user pada daerah ini tidak dapat mengakses access point manapun.



Gambar 17 Overlapping Signals menyebabkan Dead Spots

Pada gambar di atas roaming jaringan nirkabel sangat diperlukan. Perencanaan Roaming jaringan nirkabel mempertimbangkan kondisi seorang user berpindah posisi sehingga mengharuskan dia untuk berpindah access point yang diakses sehingga ada kemungkinana besar untuk kehilangan kekuatan sinyal yang dipancarkan .Perpindahan koneksi ini seharusnya tidak terlihat dan klien dapat langsung terhubung dengan access point terdekat untuk sinyal yang lebih kuat.

3.7.3 Prosedur Instalasi

Prosedur instalasi yang wajib ada.

1. Periksa apakah koneksi kabel yang digunakan sudah cocok. Pemasangan kabel dari access point ke switch apakah kabel UTP yang digunakan berjalan dengan baik dan benar dipasangnya.Periksa juga kabel yang digunakan untuk access point ke antena. Diperiksa terlebih dahulu apakah kabel yang digunakan sudah tepat. Diberikan label pada kabel supaya mudah dalam melakukan pemeriksaan atau dokumentasi jaringan sehingga mudah untuk melacak posisi kabel yang ingin diperiksa.
2. Buatlah desain setingan konfigurasi terlebih dahulu sebelum melakukan pada alat-alat yang ada (Access Point, Bridge, klien device) misalnya IP Address yang akan dipasang, SSID yang akan digunakan, user dan password login untuk administrator serta settingan parameter sekuritas yang harus disamakan supaya tidak terjadi masalah saat klien device ingin terhubung dengan access point yang ada.
3. Gunakan software-software yang dapat digunakan untuk menguji radius sinyal dari access point.Hal ini bertujuan untuk memeriksa radius dari sinyal access point dan pemeriksaan dari overlapping chanel.
4. Catat dan dokumentasikan setiap langkah konfigurasi serta contact person dari tim instalasi.Hal ini berguna apabila terjadi permasalahan di kemudian hari sehingga mudah dalam melakukan pengecekan permasalahan.

3.7.4 Penempatan Alat-Alat Jaringan Nirkabel

Akses point biasanya diletakan pada tempat atau titik yang bisa memberikan sinyal atau radius yang seluas mungkin. Penempatan akses point untuk ruangan indoor sebaiknya berada di tempat yang tidak banyak sekat atau dinding sebisa mungkin lone of sight karena radius signal akan semakin kecil apabila semakin banyak sekat atau halangan. Perlu diperhatikan juga dalam memasang access point channel yang digunakan supaya tidak terjadi dead spot atau tabrakan frekuensi.

Sedangkan untuk outdoor ,sebaiknya dilakukan site survei terlebih dahulu untuk mengecek keadaan lapangan.Jangan sampai sinyal pada titik yang akan dipasang akses point akan bertabrakan dengan akses point lain yang telah terpasang lebih dahulu dan keamannya perlu diperhitungkan.Seperti memasang di tempat yang tinggi dan dipasangi anti petir.

3.7.5 Pengkabelan

Pemasangan kabel ini dilakukan hanya untuk kabel UTP yang dihubungkan dengan akses point karena ini merupakan jaringan nirkabel sehingga yang perlu diperhatikan dalam pengkabelan adalah koneksi access point ke switch. Hal ini bertujuan untuk mengetahui apakah kabel tersebut dapat digunakan atau tidak (mis: karena isinya terputus).

Setelah kabel dipasang, gunakan pipa penutup agar rapi. Pemberian tanda pada kabel sebaiknya diterapkan agar memudahkan pengawasan ataupun perbaikan jika terjadi suatu kerusakan.

Setelah akses point diletakkan di masing-masing lokasi, maka langkah selanjutnya adalah menarik kabel, memasang kartu wireless adapter pada PC user yang akan menggunakan jaringan nirkabel dan memasang parameter sekuritas yang sama untuk setiap PC, laptop ,Handphone ataupun PDA yang akan mengakses jaringan nirkabel tersebut.

3.7.6 Proses Instalasi Jaringan Nirkabel

Sebelum dilakukan instalasi perlu dibuat sebuah jadwal pekerjaan yang baik agar proses instalasi berjalan dengan lancar. Jadwal tersebut secara sekuensial (urut) meliputi hal-hal berikut:

- Membuat desain jaringan di atas kertas sesuai dengan kondisi nyata di lapangan
- Melakukan pembongkaran dan pembenahan infrastruktur lapangan,
- Melakukan pemasangan peralatan jaringan secara menyeluruh

- Melakukan konfigurasi peralatan jaringan secara menyeluruh
- Menguji konektivitas semua node dalam jaringan dan radius dari access point yang dipasang.

3.7 Tim Instalasi

Tim instalasi adalah orang-orang yang terlibat dalam melaksanakan instalasi suatu jaringan Nirkabel. Orang-orang ini hendaknya bukanlah orang-orang sembarangan, melainkan memiliki pengalaman dalam bidang jaringan komputer, khususnya pengalaman dalam melakukan instalasi jaringan nirkabel.

Faktor yang perlu dipertimbangkan dalam pemilihan tim instalasi jaringan nirkabel adalah sebagai berikut:

- Banyak lokasi instalasi
- Kapasitas user yang akan mengakses jaringan Nirkabel

Besar biaya yang akan dikeluarkan untuk proses penginstalan jaringan.

BAB 4
Menginstal Sumber Daya Berbagi pada Jaringan Komputer

4.1 Pendahuluan

Salah satu keunggulan dengan adanya jaringan computer adalah, kita dapat memberdayakan hardware yang sama, untu semua computer yang menjadi anggota jaringan tersebut.

Sebelum resource dishare, ada beberapa factor yang harus diperhatikan:

1. Sistem Operasi

   Seperti yang kita ketahui, sistem operasi merupakan sistem yang mengatur secara keseluruhan bagaimana computer bekerja. Oleh Karena itu penting untuk mengetahui sistem operasi computer pada komputer2 yang ada di jaringan…sebab tiap sistem operasi tentu saja memiliki mekanisme yang berbeda dalam membagi resource

2. Driver, jika yang dishare berupa hardware

   Kompatibilitas hardware merupakan hal yang penting yang perlu pula diperhatikan. Driver dari hardware biasanya ditujukan hanya pada sistem operasi tertentu, oleh karena itu perlu hati2 membaca keterangan kompatibilitas driver sebelum melakukan proses penginstalan

3. Security

   Pengaturan penggunaan resource juga perlu ada, agar tidak digunakan seenaknya.

Sumber daya yang hendak dishare biasanya disambungkan ke salah satu computer dalam jaringan (biasanya server), atau menggunakan hub – hub khusus untuk menshare beberapa hardware sekaligus.

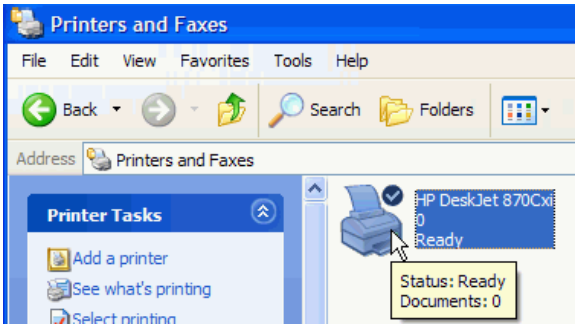
4.2 Konfigurasi Sumber Daya Pakai

Pada bagian ini akan dibahas beberapa cara untuk melakukan sharing pada beberapa resource yang lazim dishare dalam sebuah network..

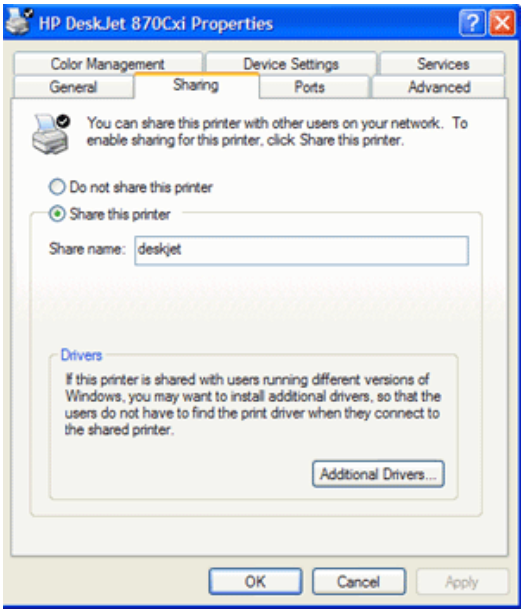
1. Printer

   Cara paling mudah untuk menshare printer adalah dengan menghubungkannya dengan salah satu computer, kemudian melakukan langkah2 sebagai berikut (OS Windows XP)

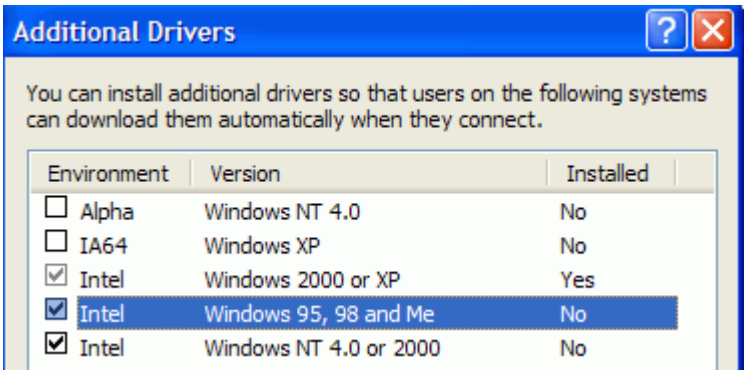
- Di sudut kiri bawah, klik tombol **start→Control Panel** lalu cari tombol **Printer and Faxes**, kemudian akan muncul layar seperti di bawah ini:



- Kemudian klik kanan pada printer anda, dan klik sharing, sehingga muncul jendela seperti gambar ini



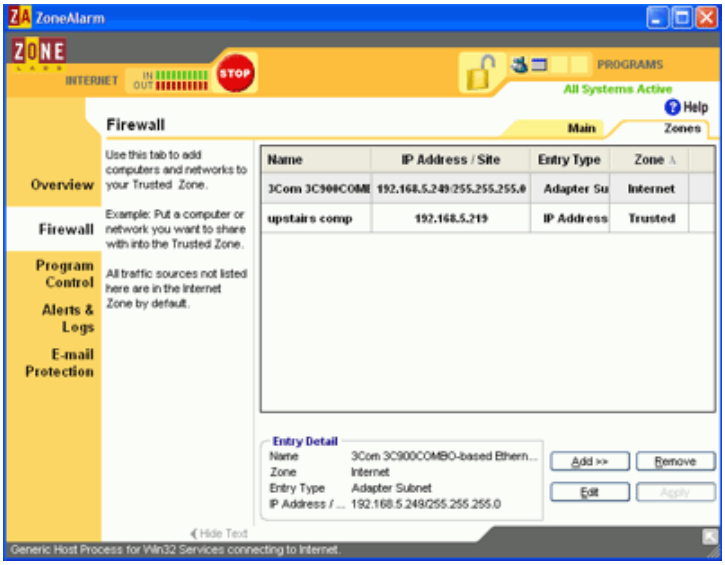
- Pilih share this printer dan tentukan namanya, lalu klik Additional Drivers, lalu akan keluar layar seperti berikut:



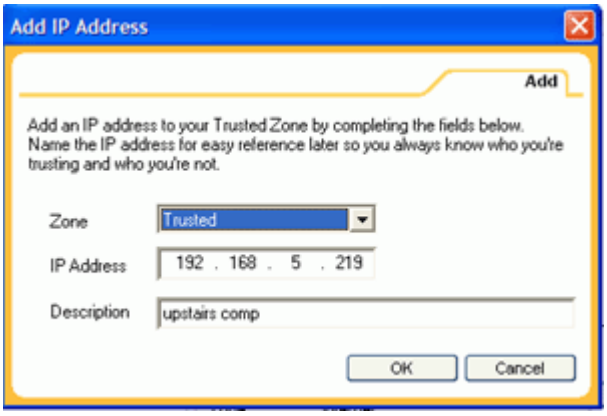
Fitur ini berfungsi untuk mengantisipasi bila ada komputer2 pada jaringan menggunakan sistem OS yang berbeda. Klik sesuai dengan OS yang ada di jaringan

- Konfigurasi firewall juga perlu diperhatikan, sebab secara default, firewall memblok fitur sharing printer….oleh karena itu, perlu dibuka agar sharing bias dilakukan. Di sini akan dibahas dua firewall yang paling sering digunakan,yakni Zone Alarm dan firewall Windows XP sendiri
- **Zone Alarm**

  Buka ZoneAlarm dan klik Zones, seperti gambar di bawah ini



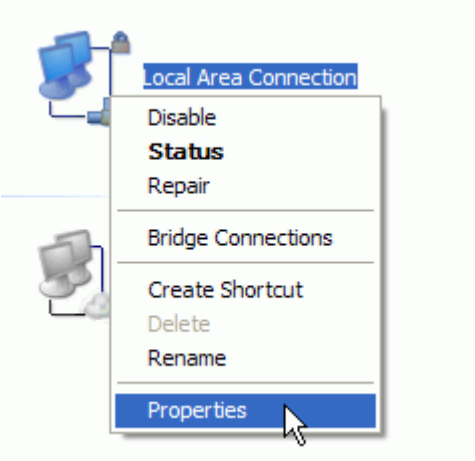
Lalu pilih ‘add, lalu IP Adddress’ maka akan tampil seperti berikut



Pastikan zone yang dipilih adalah trusted, dan tulis IP address dari computer yang ada di jaringan. Ulangi prosedur ini untuk semua computer di jaringan agar semuanya dapat menggunakan shared printer. IP address bias disesuaikan tergantung computer mana saja yang boleh menggunakan printer sharing.

- Windows XP Firewall

  Buka kembali **control panel**, lalu klik **Network Connections**… bila LAN anda terdapat gambar gembok seperti di bawah ini, maka berarti firewall Windows dinyalakan, oleh karena itu, klik kanan dan pilih **Properties** untuk mengkonfigurasi



Lalu klik tab **Advanced** , klik **Settings** dan matikan firewallnya….

4.3 Konfigurasi Security printer pada computer Server

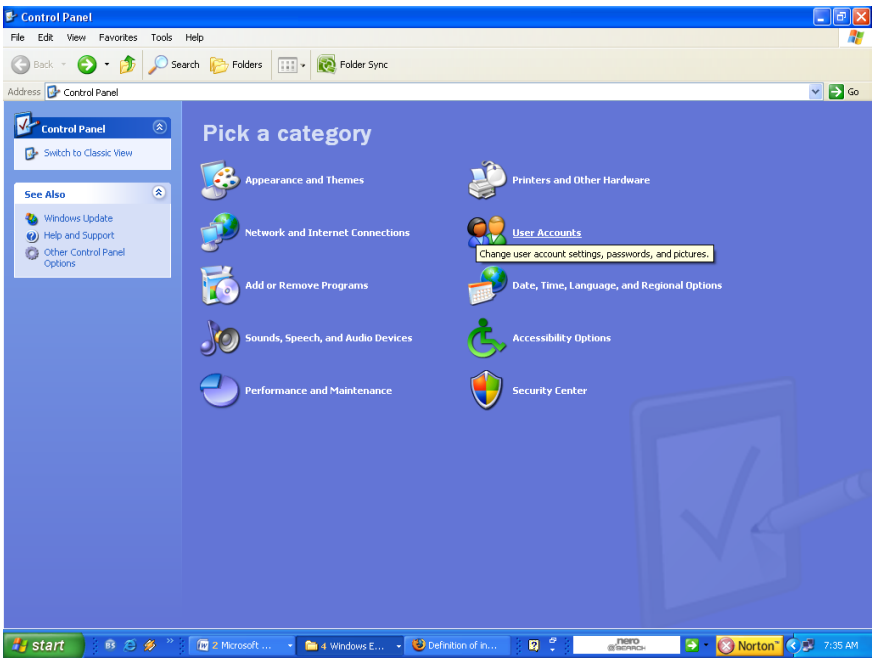
Yang dimaksud dengan computer server di sini adalah computer yang dipasangkan printer. Seperti yang telah disebutkan di bab pendahuluan…Security merupakan hal yang penting dalam mengatur ketertiban penggunaan sumber daya jaringan…

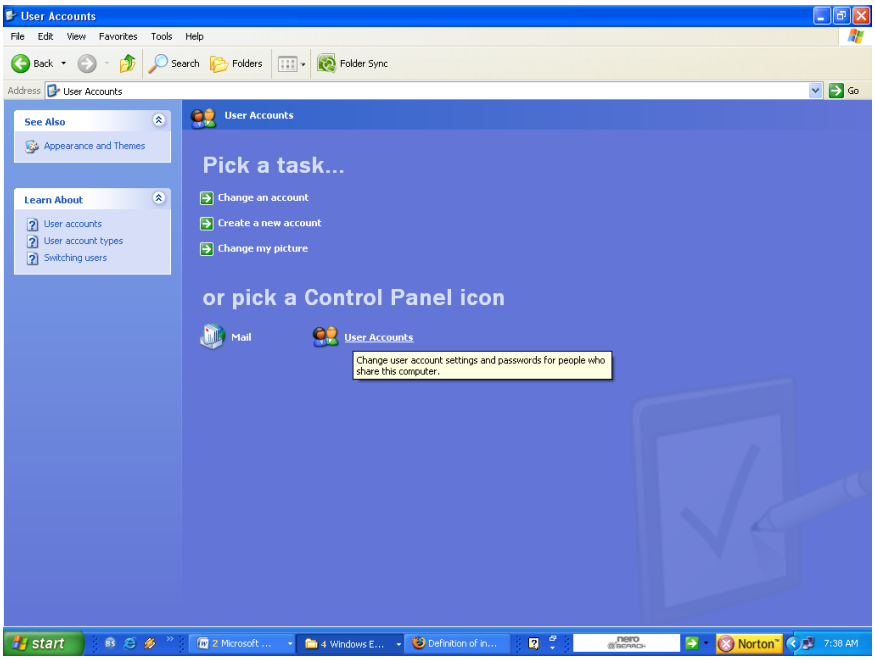
Ada dua cara pengaturan hak akses printer pada windows XP.

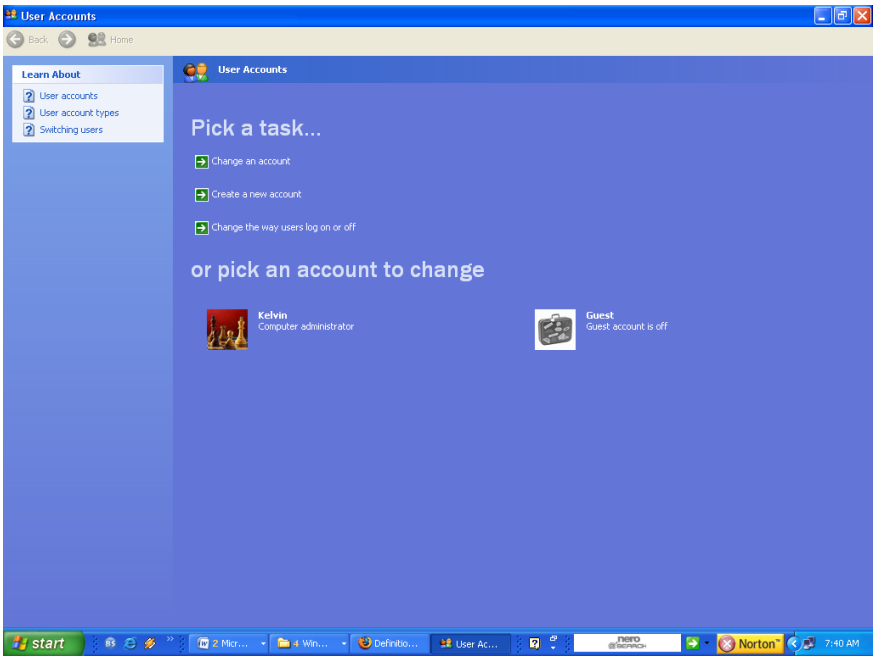
1. Bila semua user tanpa terkecuali memiliki hak yang sama untuk memakai printer, maka, cukup membuat account guest pada server..yakni dengan cara:

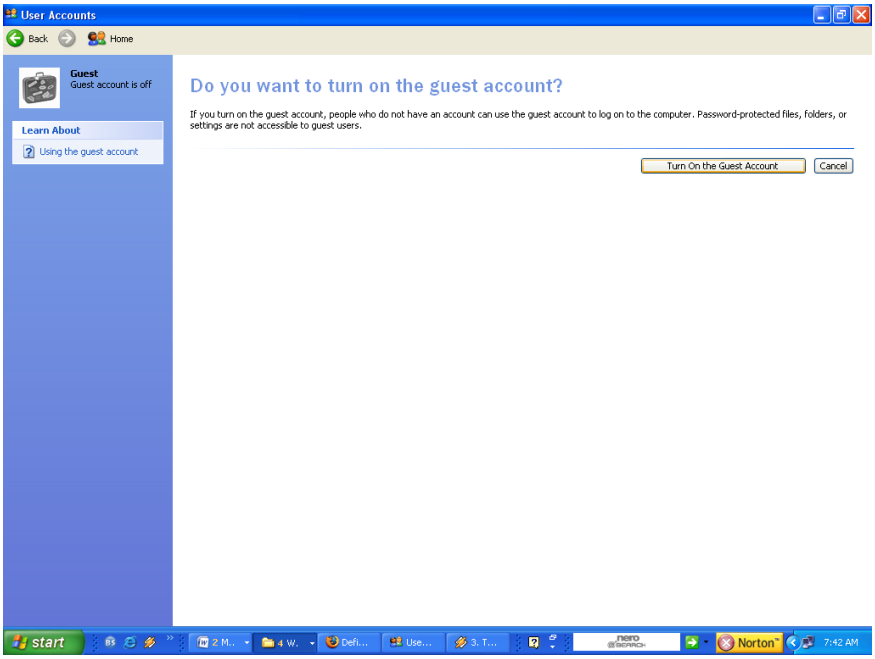
   Start→User Accounts→Click Account Guest→nyalakan, lebih lanjut dapat dilihat pada gambar berikut:

1.




User Accounts
File Edit View Favorites Tools Help
Back Search Folders Folder Sync
Address User Accounts
Go
See Also
Appearance and Themes
Learn About
User accounts
User account types
Switching users
User Accounts
Pick a task...
Change an account
Create a new account
Change my picture
or pick a Control Panel icon
Mail
User Accounts
Change user account settings and passwords for people who share this computer.
start
Norton
7:38 AM


User Accounts
Back Home
Learn About
User accounts
User account types
Switching users
User Accounts
Pick a task...
Change an account
Create a new account
Change the way users log on or off
or pick an account to change
Kelvin
Computer administrator
Guest
Guest account is off
start
Norton
7:40 AM



2. Di setiap komputer di jaringan dibuat user accounts, caranya sama dengan di atas…..kemudian di server dibuat juga user account sesuai dengan user account – user account yang ada di computer lain.

Pada sistem operasi Windows Server 2003, sistem security dan manajemen pemakai sumber dayanya lebih lengkap dan aman, sebab Windows Server menyediakan fitur berupa Domain Policy dan Active Directory, prosedurnya miri dengan pada Windows XP, hanya saja pada tab Sharing nantinya akan ada juga Permissions, sehingga user bisa ditambahkan langsung.

4.6 Sharing File dan Scanner

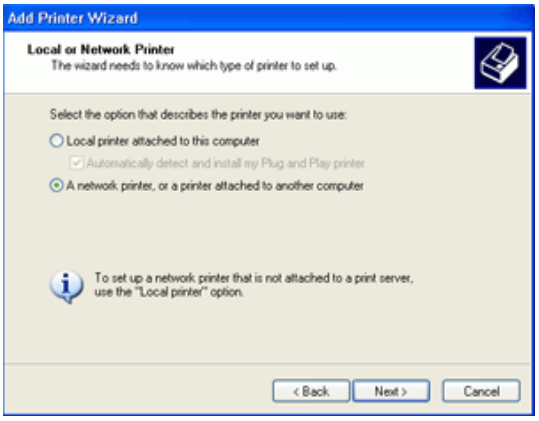
Sharing File memiliki prosedur yang hampir sama dengan sharing printer, hanya saja klik kanan dilakukan pada folder yang hendak dishare, dan diatur sharingnya sama seperti sharing printer.

Penggunaan oleh User:

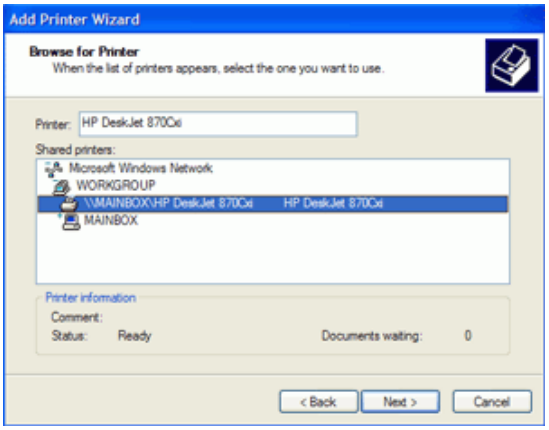
Konfigurasi pada user cukup sederhana, yakni:

- Setelah konfigurasi ini selesai, sekarang di computer – computer lain dilakukan setting seperti ini:

  Start→Control Panel→Printers and Faxes→Klik kanan lalu pilih **Add Printer** maka akan muncul jendela seperti berikut.



Pilih option kedua, karena kita akan menggunakan printer dalam jaringan, setelah itu klik **Next,** setelah itu pilih browse for a printer. Komputer akan mencari printer yang ada di dalam jaringan, lalu pilihlah printer yang dimaksud, seperti gambar berikut:

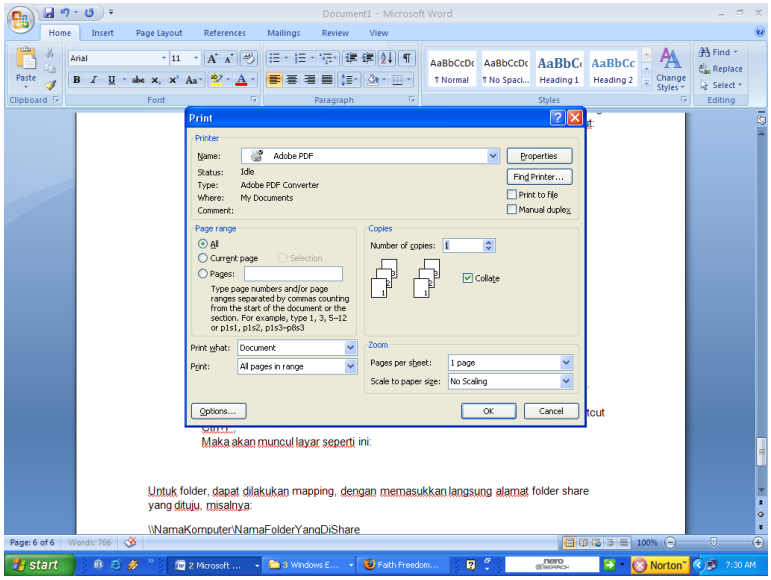


Printer sekarang siap digunakan…..

Perlu diingat bahwa printer hanya dapat digunakan bila user account yang digunakan cocok dengan user account yang ada di server, sehingga user perlu meminta pada server admin untuk menambahkan user account pada servernya.

Bila printer hendak digunakan, misalnya dengan office, maka tekan tombol shortcut Ctrl+P,

Maka akan muncul layar seperti ini:

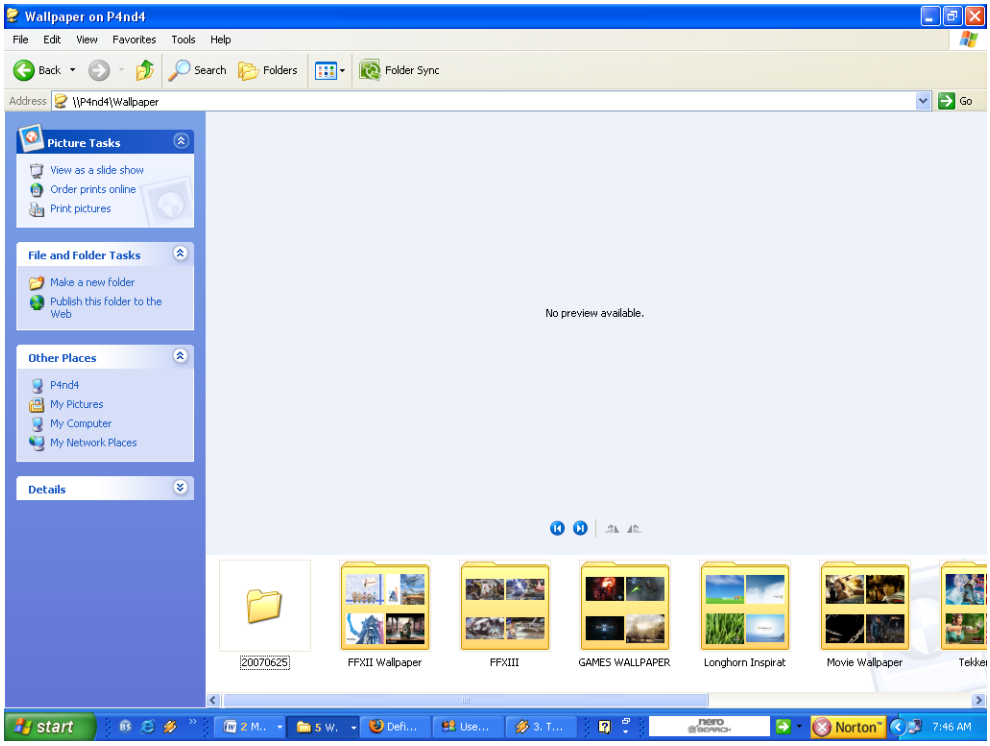


Pilih printer sharing di kolom Name. Lalu diprint seperti biasa

Untuk folder, dapat dilakukan mapping, dengan memasukkan langsung alamat folder share yang dituju, misalnya:

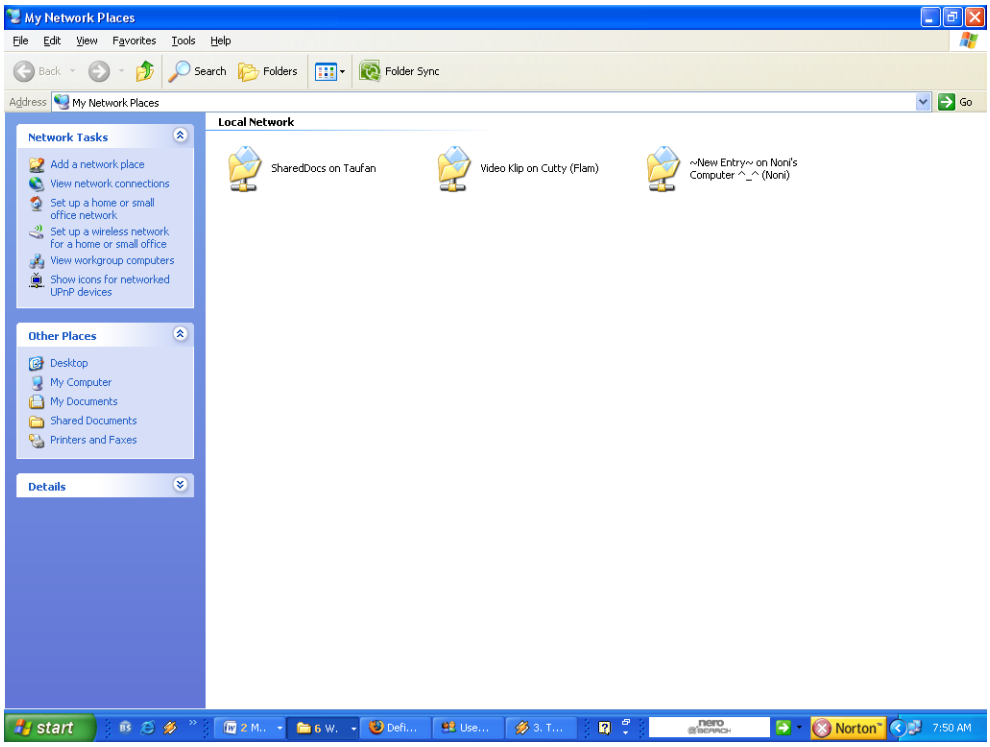
\\NamaKomputer\NamaFolderYangDiShare

Contohnya dapat dilihat pada gambar ini.

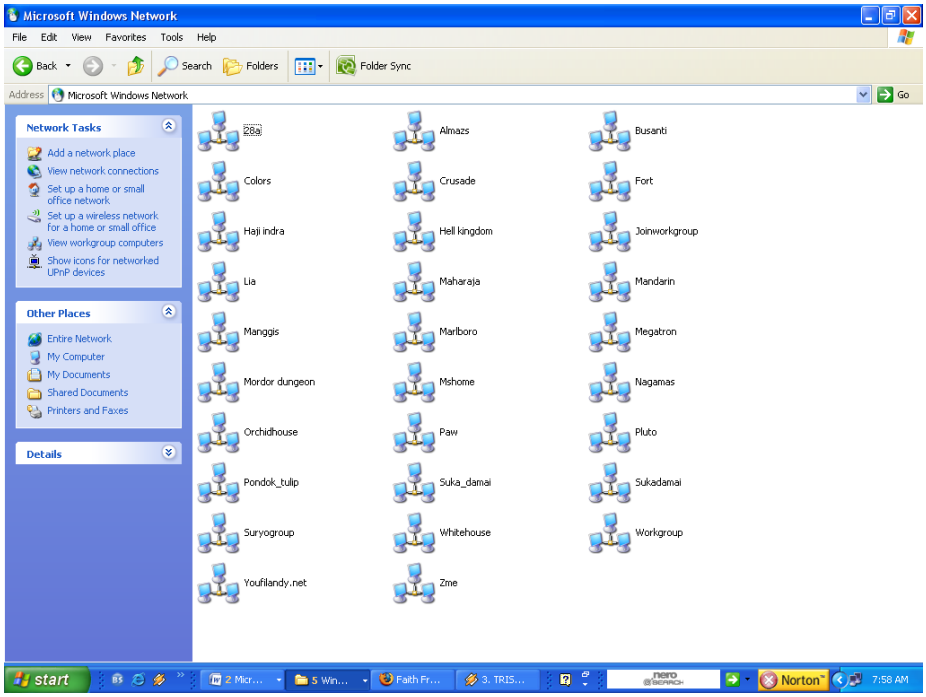


Bila alamat tidak diketahui maka kita dapat menggunakan fasilitas dari windows, yaitu **My Network Places**

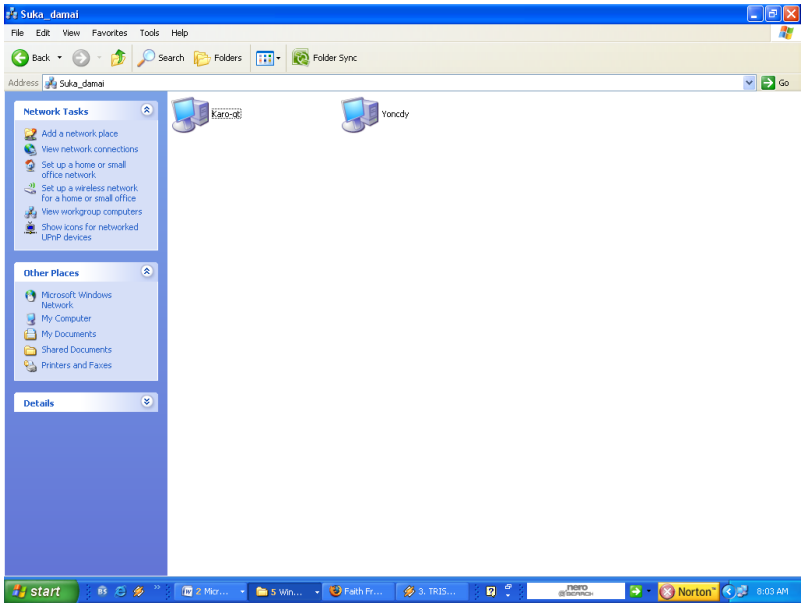
Klik Start→My Network Places, lalu akan muncul jendela seperti ini:



Perhatikan folder – folder yang ada pada jendela ini merupakan folder sharing yang pernah dikunjungi dan berhasil diakses sebelumnya. Folder – folder ini berfungsi sebagai shortcut bila source yang sama hendak dibrowse kembali… Langkah selanjutnya…perhatikan bagian kiri pilih Microsoft Windows Network, maka akan keluar layar seperti ini:



Gambar komputer menunjukkan group – group yang ada di dalam jaringan tersebut. Anda tinggal memilih dan mencari letak computer yang dimaksud.



BAB 5
Menyelenggarakan Administrasi Sistem Jaringan

5.1 Uraian Singkat Materi

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah:

- Membagi sumber daya: contohnya berbagi pemakaian printer, CPU, memori, harddisk
- Komunikasi: contohnya surat elektronik, *instant messaging*, *chatting*
- Akses informasi: contohnya *web browsing*

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta layanan disebut klien (*client*) dan yang memberikan layanan disebut pelayan (*server*). Arsitektur ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Klasifikasi Berdasarkan skala :

- Local Area Network (LAN)
- Metropolitant Area Network (MAN)
- Wide Area Network (WAN)

Berdasarkan fungsi : Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai client dan juga server. Tetapi ada jaringan yang memiliki komputer yang khusus didedikasikan sebagai server sedangkan yang lain sebagai client. Ada juga yang tidak memiliki komputer yang khusus berfungsi sebagai server saja. Karena itu berdasarkan fungsinya maka ada dua jenis jaringan komputer:

- Client-server

Yaitu jaringan komputer dengan komputer yang didedikasikan khusus sebagai server. Sebuah service/layanan bisa diberikan oleh sebuah komputer atau lebih. Contohnya adalah sebuah domain seperti www.detik.com yang dilayani oleh banyak komputer web server. Atau bisa juga banyak service/layanan yang diberikan oleh satu komputer. Contohnya adalah server jtk.polban.ac.id yang merupakan satu komputer dengan multi service yaitu mail server, web server, file server, database server dan lainnya.

- Peer-to-peer

Yaitu jaringan komputer dimana setiap host dapat menjadi server dan juga menjadi client secara bersamaan. Contohnya dalam file sharing antar komputer di Jaringan

Windows Network Neighbourhood ada 5 komputer (kita beri nama A,B,C,D dan E) yang memberi hak akses terhadap file yang dimilikinya. Pada satu saat A mengakses file share dari B bernama data_nilai.xls dan juga memberi akses file soal_uas.doc kepada C. Saat A mengakses file dari B maka A berfungsi sebagai client dan saat A memberi akses file kepada C maka A berfungsi sebagai server. Kedua fungsi itu dilakukan oleh A secara bersamaan maka jaringan seperti ini dinamakan peer to peer.

Berdasarkan topologi jaringan : Berdasarkan (topologi jaringan), jaringan komputer dapat dibedakan atas:

- Topologi bus
- Topologi bintang
- Topologi cincin

5.2 Beberapa Pengertian dalam Unit Kompetensi Ini

Beberapa pengertian yang dipergunakan di dalam unit kompetensi ini, yaitu :

a. *Password*, adalah suatu bentuk data autentik rahasia yang digunakan oleh *user* ketika akan menjalankan suatu program atau situs yang tidak ingin atau tidak dapat dirubah atau dilihat semua orang/orang lain (bersifat rahasia).
b. kriptografi, adalah ilmu untuk menjaga kerahasiaan berita/informasi.
c. topologi adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node, link, dan station.*
d. Access Control Lists (ACLs), adalah daftar dari kendali akses yang menunjukkan hak akses dan informasi untuk audit yang digunakan oleh sistem, misalnya oleh Windows NT atau oleh proxy server. Didalam Windows NT, ACLs ini akan digunakan bersama-sama dengan sistem akses file sytem NTFS (*New Technology File System*). Windows NT menggunakan daftar ini untuk melihat siapa saja yang telah diberikan hak untuk mengakses sumber daya tertentu (*file* atau *folder*) dan hak apa yang telah diberikan kepadanya, seperti membaca, menulis dan mengeksekusi. Didalam sistem file UNIX, hak akses ini dapat dilihat dari bit-bit kode akses yang meliputi akses untuk *user*, akses untuk *group user* serta akses untuk *global user*. Akses untuk *user* berlaku untuk *user* yang besangkutan, akses untuk *group user* berlaku untuk *user-user* lain yang masih berada dalam satu group dengan *user* yang bersangkutan sedangan akses *global user* berlaku untuk *user* yang tidak berada dalam satu *group* dengan *user* yang bersangkutan. Setiap file dalam file sistem UNIX memiliki bit-bit pengendali tersebut.
e. Challenge/Response, adalah Proses otentifikasi melibatkan prosedur *challenge/response* yang terjadi pada saat dimulainya sebuah otentifikasi. Ketika seorang pemakai ingin meminta hak akses kepada sistem maka sistem akan mengirimkan challenge kepada pemakai kemudian pemakai mengirimkan kode yang sesuai. Sistem akan membandingkan kode yang dikirimkan oleh pemakai dengan kode yang ada didalam database. Jika ada kecocokan maka sistem akan memberikan hak akses sesuai dengan hak yang dimiliki oleh pengguna yang bersangkutan. Contohnya, pada saat seorang administrator

   Web ingin mengakses IIS (*Internet Information Service*) di Windows NT maka proses *challenge/response* terjadi agar sistem dapat memberikan hak akses yang sesuai. Contoh lain dalam sistem UNIX yang menggunakan *one-time password*, seorang pemakai yang ingin melakukan koneksi terminal (telnet) ke dalam sistem harus memasukkan *password* sebelum sistem memberikan hak akses terhadap terminal. Proses *challenge/response* yang terjadi disini yaitu pemakai

menghubungi server melalui port telnet (21), kemudian server membentuk hash serta *challenge key*. Pemakai kemudian membalas *challenge key* tersebut dengan *one-time-password* yang sesuai. Selanjutnya *response*/jawaban dari pemakai akan dibandingkan dengan database yang ada didalam sistem, sebelum diputuskan untuk memberikan akses atau tidak.

f. NTLM, adalah NTLM adalah teknik otentifikasi Challenge/Response yang digunakan oleh Window NT. NTLM singkatan dari Windows NT LAN Manager, sebab teknik ini dikembangkan pertama kali dan digunakan oleh Microsoft LAN Manager

g. *One-Time-Password* adalah teknik otentifikasi Challenge/Response yang sering digunakan oleh UNIX system. Dengan teknik ini sebuah *password* hanya dapat digunakan satu kali dimana response yang sesuai akan diminta oleh sistem, berdasarkan challenge key yang diberikan pada saat proses otentifikasi.

h. SAM atau kepanjangan dari *Security Account Manager* adalah database yang berisi data pemakai dan group. SAM tidak menyimpan *password* dalam bentuk ASCII tetapi dalam bentuk hash. SAM digunakan oleh

Windows NT dan terletak di HKEY_LOCAL_MACHINE\SAM dan HKEY_LOCAL_MACHINE\Security\SAM

Hash dalam keamanan jaringan

Dalam sebuah sistem terbuka, dimana komunikasi berlangsung melewati beberapa, ratusan bahkan ribuan komputer lainnya yang terhubung dalam jaringan maka pengiriman data dari satu tempat ke tempat lainnya akan sangat rawan terhadap penyadapan. Bagaimana jika hal ini terjadi sesaat sebelum proses otentifikasi berlangsung. Seorang '*sniffer*' (penyadap data yang dikirimkan melalui internet) dapat mengendus *password* dan nama pemakai yang dikirimkan melalui jaringan. Untuk mengatasi hal ini maka dibuatlah algoritma hash, dimana *password* akan tersimpan dalam bentuk lain setelah diproses melalui algoritma hash tersebut. Algoritma standar *hash* yang sering digunakan adalah MD4 yang akan menghasilkan 16 byte (128 bit) hash, atau dengan kata lain, berapapun panjang bit yang dimasukkan dalam algoritma ini, maka panjang bit keluaran hasil hash adalah 16 byte (128 bit). Secara teoritis sangatlah tidak mungkin untuk menggabungkan hash dan algoritma yang dipakai serta kemudian melakukan proses revers secara matematis untuk memperoleh *password* yang bersesuaian. Atau dengan kata lain, proses hash hanya berlangsung satu arah dan bukan proses yang dapat dibalik.

Enkripsi dalam keamanan jaringan

Selain beberapa definisi serta teknik yang disebutkan diatas, salah satu teknik yang sangat penting adalah enkripsi. Coba bayangkan pada saat kita melakukan koneksi terminal (telnet , port 21) pada jaringan kita dari Jakarta ke Surabaya melalui Internet yang notabene melalui ratusan bahkan ribuan router. Dalam

spesifikasinya, komunikasi terminal tersebut mentransmisikan data-data dalam bentuk text ASCII. Jika kemudian ada seorang sniffer yang mengendus data-data

yang ditransmisikan antara komputer server dengan terminal kita maka data-data tersebut akan dengan mudah terbaca. Jika kemudian kita membaca email yang ada dalam server kita, maka *sniffer* tadi juga dapat ikut membaca email yang kita baca.

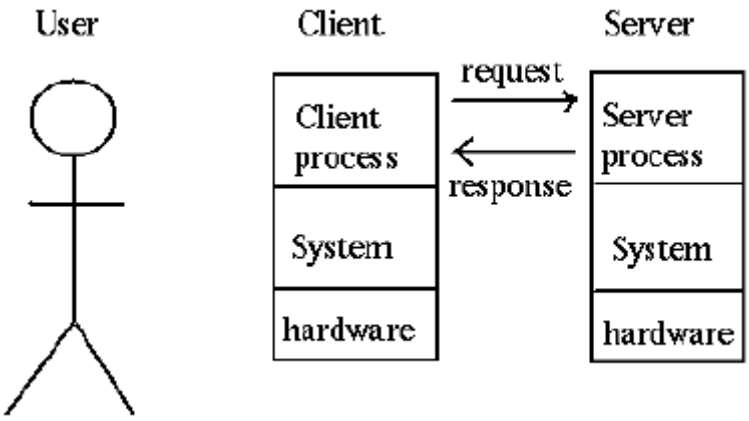
Untuk mengatasi hal tersebut diatas maka diciptakan sistem enkripsi dimana data-data yang dikirimkan sudah dalam bentuk terenkripsi. Untuk melakukan enkripsi dibutuhkan kunci pembuka yang harus diketahui oleh server dan pengguna. Akan tetapi jika seorang sniffer dapat mengendus kunci pembuka tersebut, maka dia juga dapat membuka data-data komunikasi antara pemakai dan server. Oleh karena itu diciptakan teknik enkripsi dengan kunci publik dari RSA, dimana kunci publik dapat disebarluaskan secara bebas, sementara kunci privat disimpan secara rahasia. Seorang pemakai yang ingin melakukan koneksi kemudian memberikan kunci publiknya kepada server serta mengambil kunci publik server. Pengguna yang bersangkutan kemudian melakukan enkripsi dengan kunci privat miliknya serta kunci publik milik server kemudian mengirimkan data tersebut kepada server. Server kemudian melakukan de enkripsi dengan menggunakan kunci privat miliknya serta kunci publik milik pengguna yang bersangkutan. Dengan demikian meskipun data dapat diendus oleh sniffer, namun data tersebut tidak dapat diintepretasikan dengan baik dan benar.

Mendokumentasikan Akses Keamanan
Client-Server
Pengertian Client Server

Client-server adalah arsitektur jaringan yang memisahkan client (biasanya aplikasi yang menggunakan GUI) dengan server. Masing-masing client dapat meminta data atau informasi dari server.

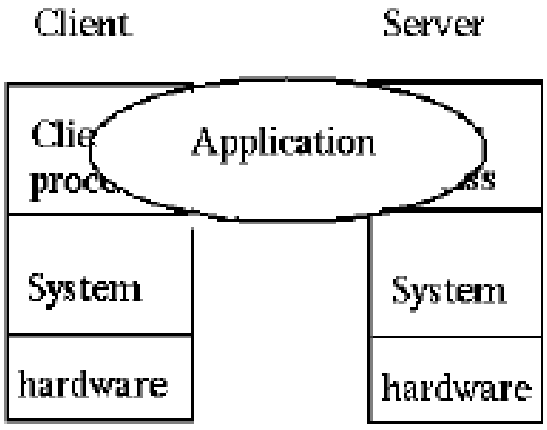
Sistem client server didefinisikan sebagai sistem terdistribusi, tetapi ada beberapa perbedaan karakteristik yaitu :

1. Servis (layanan)
   - Hubungan antara proses yang berjalan pada mesin yang berbeda
   - Pemisahan fungsi berdasarkan ide layanannya
   - Server sebagai provider, client sebagai konsumen
2. Sharing resources (sumber daya)
   - Server bisa melayani beberapa client pada waktu yang sama, dan meregulasi akses bersama untuk share sumber daya dalam menjamin konsistensinya.
3. Asymmetrical protocol (protokol yang tidak simetris)
   - *Many to one relationship* antara client dan server. Client selalu menginisiasi dialog melalui layanan permintaan dan server menunggu secara pasif request dari client.
4. Transparansi lokasi
   - Proses yang dilakukan server boleh terletak pada mesin yang sama atau pada mesin yang berbeda melalui jaringan. Lokasi server harus mudah diakses dari client.
5. Mix-and Match
   - Perbedaan server client platforms
6. Pesan berbasiskan komunikasi
   - Interaksi server dan client melalui pengiriman pesan yang menyertakan permintaan dan jawaban.
7. Pemisahan interface dan implementasi
   - Server bisa diupgrade tanpa mempengaruhi client selama interface pesan yang diterbitkan tidak berubah.



Gambaran Client Server System (Elemen Kompetensi 1)

Client Server Application



Gambaran Client/Server Application (Elemen Kompetensi 1)

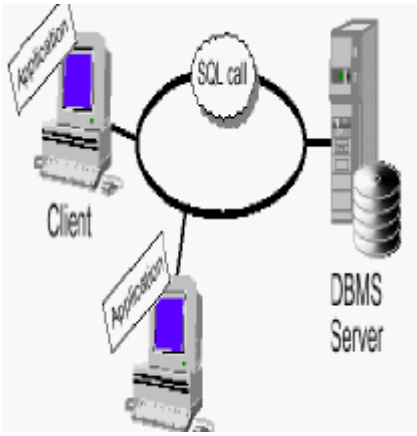
Perbedaan tipe Client-Server :

1. File Servers
   - File server vendors mengklaim bahwa mereka pertama kali menemukan istilah client-server.
   - Untuk sharing file melalui jaringan

Gambaran Topologi untuk File Servers

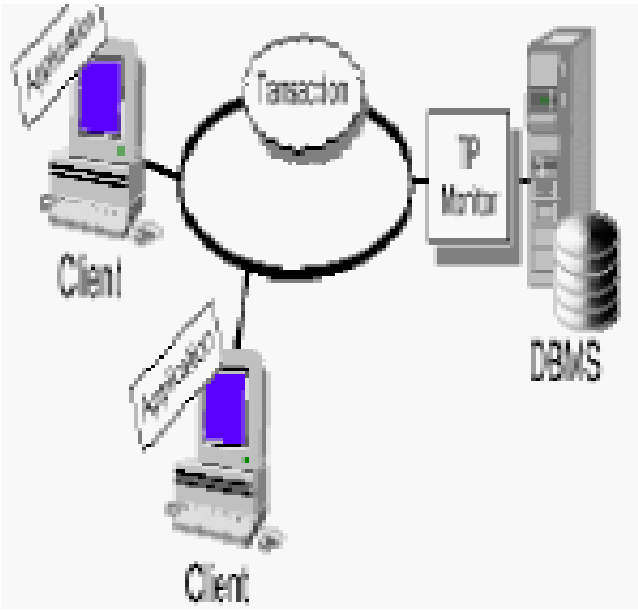
2. Database Servers
   - Client mengirimkan SQL *request* sebagai pesan server, selanjutnya hasil perintah SQL dikembalikan.

- Server menggunakan kekuatan proses yang diinginkan untuk menemukan data yang diminta dan kemudian semua record dikembalikan pada client.



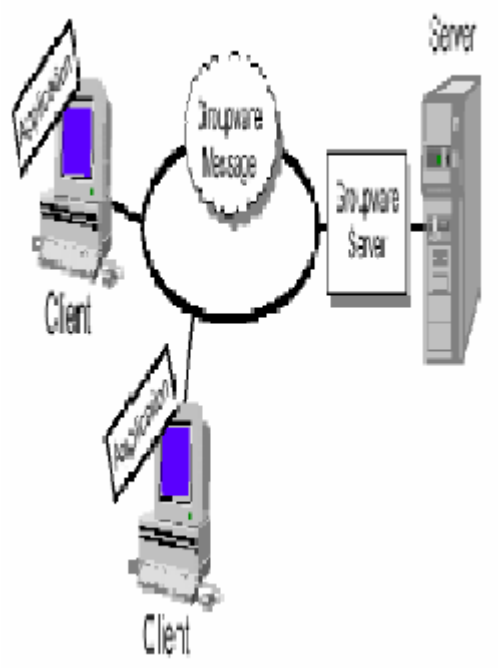
Gambaran Topologi untuk Database Servers

3. Transaction Servers (Transaksi Server)
   - Client memiliki remote procedures yang terletak pada server dengan sebuah SQL database engine.
   - Remote procedures ini mengeksekusi sebuah grup dari SQL statement.
   - Hanya satu permintaan/jawaban yang dibutuhkan untuk melakukan transaksi.



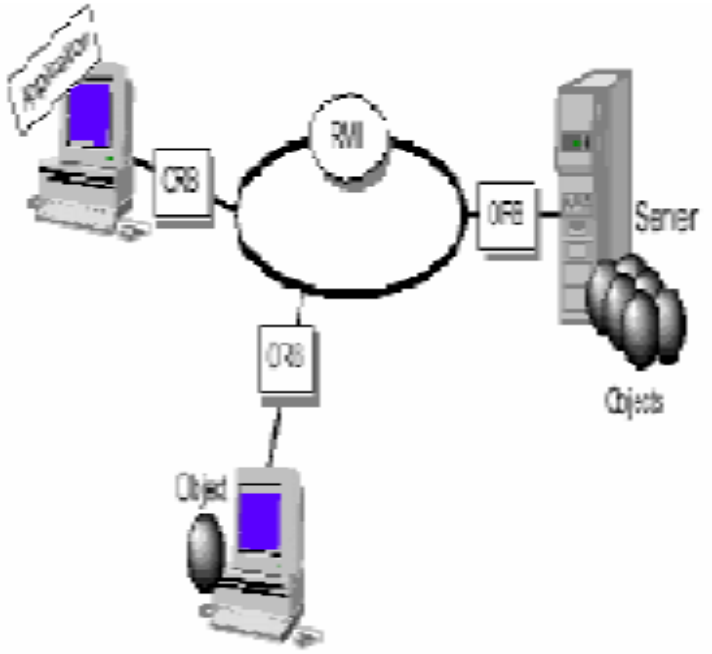
Gambaran Topologi Transaksi Server

4. Groupsware Servers
   - Dikenal sebagai *computer suppoted cooperative working*
   - Manajemen semi struktur informasi seperti teks, image, buletin boards, dan aliran kerja.
   - Data diatur sebagai dokumen



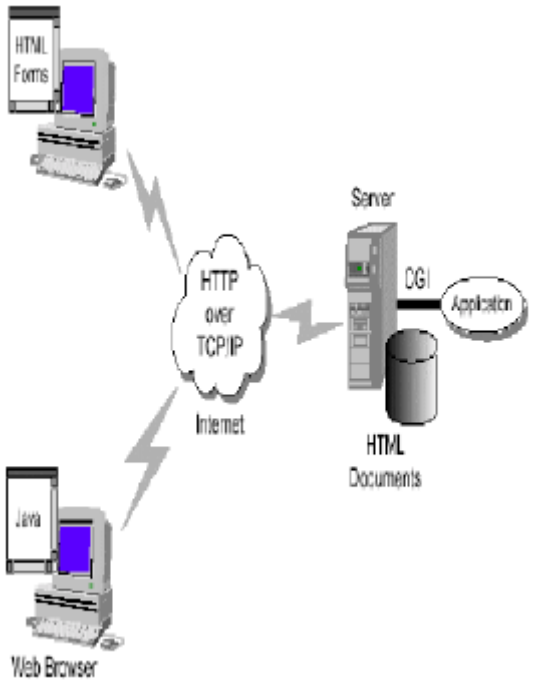
Gambaran Topologi Groupsware Servers

5. Object Application Servers
   - Aplikasi client/server ditulis sebagai salah satu set objek komunikasi.
   - Client object berkomunikasi dengan server objects melalui *Object Request Broker (ORB)*
   - Client meminta sebuah method pada remote object



Gambaran Topologi Object Application Servers

6. Web Application Servers (Aplikasi Server)
   - World Wide Web adalah aplikasi client server yang pertama yang digunakan untuk web.
   - Client dan servers berkomunikasi dengan menggunakan RPC sebagai protokol yang disebut HTTP.



Gambaran Topologi Web Application Servers

Proses Perancangan Sistem Informasi

Proses perancangan aplikasi sistem informasi berbasis web memerlukan analisis menyeluruh tidak hanya sebatas pada fungsionalitas sistem saja, tetapi juga prosedur untuk menjaga kerahasiaan data dan informasi. Pentingnya kerahasiaan data ini membutuhkan adanya proses identifikasi atau otentikasi terhadap user yang akan menggunakan sistem, hal ini untuk memastikan apakah seseorang berhak atau tidak untuk mengakses data dan informasi.

Data penting yang dikelola oleh aplikasi memungkinkan adanya ancaman terhadap kerahasiaan data tersebut. Ancaman ini salah satunya bisa datang dari hacker yaitu orang yang mampu menembus proteksi pengendali akses dalam sebuah sistem, dengan memanfaatkan celah/kelemahan sistem tersebut. Seorang hacker dapat menembus sistem dan mengakses data layaknya seorang yang diberi hak akses, yakni dengan menungkap username dan *password* login dari orang-orang yang berhak tersebut.

Permasalahan yang dijumpai hampir pada setiap aplikasi yang menyimpan data penting ini memerlukan adanya kontrol akses untuk mencegah akses yang tidak berhak ke objek, data dan informasi yang sensitif. Salah satu jenis serangan terhadap media kontrol akses adalah brute force attack. Metode serangan ini sebenarnya bukanlah cara baru, yakni metode coba-coba (trial and error) yang dilakukan oleh penyerang menggunakan tool atau script penebak *password* yang dapat bekerja efektif untuk mendapatkan otentikasi yang dianggap valid oleh sistem. Brute force attack dapat dilakukan dengan menebak *password* dari sebuah username dengan mencoba semua kombinasi karakter yang mungkin untuk memperoleh akses yang valid.

Salah satu turunan brute force attack ialah dictionary attack yang dilakukan dengan mencoba memberikan *password* berupa kata-kata yang umum digunakan dan mudah untuk dicari dari sebuah daftar atau kamus. Hal ini sangat mungkin dilakukan karena pada kenyataannya, banyak user yang mengunakan *password* login dengan kata-kata yang mudah ditebak.

Cara termudah untuk menghindari serangan ini yaitu dengan menerapkan kebijakan *password* yang ketat, misalnya user tidak diperbolehkan membuat *password* dengan karakter yang sama atau menyerupai dengan username, atau menggunakan kata-kata yang mudah ditebak. Pengembang aplikasi juga harus mengindari tampilan informasi tentang username dan *password* login seperti memberikan komentar "invalid username" atau "invalid *password*", karena hal ini memudahkan penyerang untuk menemukan username yang cocok dan kemudian melakukan brute force attack.

Pengaturan server untuk membatasi akses dari sebuah IP address tertentu yang mencoba melakukan brute force attack juga dapat dilakukan untuk mengurangi kemungkinan terjadinya serangan. Server harus dapat memblokir akses dari sebuah host yang telah beberapa kali gagal melakukan login pada saat yang berurutan atau diindikasikan sebagai brute force attack.

Teknik lain untuk menghindari kemungkinan terjadinya brute force attack yaitu dengan menambahkan fungsi untuk membuat sebuah bilangan dan/atau karakter acak yang harus dimasukkan oleh user ketika akan melakukan login ke dalam sistem, selain memasukkan username dan *password*. Bilangan dan/atau karakter acak ini dibangkitkan oleh aplikasi dengan menggabungkan konsep session yang bekerja di sisi server,

kemudian ditampilkan dalam halaman website berupa gambar, sehingga teknik ini dapat disebut sebagai image security code.

Kode yang dibangkitkan oleh server merupakan one-time code, artinya kode tersebut hanya bekerja satu kali saja untuk satu user dalam satu session yang sedang aktif. Kode tersebut ditampilkan bersama form login dalam format gambar, bukan teks. Gambar tersebut dapat dibuat dengan menggunakan server-side scripting, misalnya PHP maupun ASP.

User harus memasukkan pasangan username, *password* dan image security code yang ditampilkan dengan benar. Apabila user telah memasukkan username dan *password* yang valid, namun image security code yang dimasukkan tidak sesuai, maka sistem akan menolak akses tersebut. Ketika user mengulangi proses ini, maka server akan membangkitkan image security code baru.

Adanya one-time code berupa gambar ini dapat memberikan jaminan keamanan data pada aplikasi dari ancaman brute force attack maupun ancaman sejenisnya. Secara tidak langsung, teknik ini dapat memastikan bahwa request berupa username dan *password* yang dikirimkan ke server adalah benar-benar diisikan oleh manusia, bukan oleh tool atau script tertentu.

Paparan di atas hanya menguraikan satu dari sekian banyak kemungkinan serangan yang dapat mengancam keamanan data pada aplikasi, karena masih banyak metode serangan lain yang juga membahayakan, misalnya SQL injection, cross site scripting, parameter manipulation, file inclusion bahkan server-side code injection. Hacker tidak akan pernah berhenti mencari celah lubang keamanan untuk memperoleh otentikasi terhadap data dan informasi yang tersimpan dalam sistem dan hal ini tentunya harus diantisipasi oleh pengembang aplikasi sejak proses perancangan sistem.

Jaringan komputer atau yang dikenal dengan internet merupakan sistem terbuka (*open system*) dimana semua orang dapat masuk ke komputer milik orang lain yang terhubung di dalam internet. Sistem terbuka juga mensyaratkan bahwa tidak ada 'batasan' bagi orang lain untuk masuk ke dalam jaringan kita, misalnya dengan menggunakan *web browsing*, akses *ftp* dan lain sebagainya.

Akan tetapi permasalahan akan timbul jika orang yang masuk ke dalam jaringan kita mempunyai maksud yang kurang baik. Seorang kompetitor misalnya, dapat saja masuk ke dalam jaringan komputer saingannya dengan tujuan mengubah sistem yang dimiliki saiangannya agar tidak dapat berfungsi dengan baik, mencuri data-data pelanggan saingan, mencuri data statistik dan lain sebagainya. Oleh karena itu dibutuhkan otentifikasi dan pengendalian akses ke dalam sistem. Secara sederhana sebuah prosedur otentifikasi adalah prosedur pengenalan jati diri seorang pemakai kepada sistem dan pemberian kartu hak akses tertentu dari sistem kepada pemakai yang bersangkutan. Seorang pemakai yang telah melewati proses otentifikasi tertentu akan memiliki hak akses tertentu dan tentu saja selalu dapat diawasi dan dikendalikan oleh sistem. Tulisan berikut ini akan memberikan dasar-dasar mengenai otentifikasi dan definisi-definisi yang berkaitan dengan keamanan jaringan.

5.3 Informasi Tiap-Tiap Elemen Kompetensi

1. Mencatat Hak Akses Keamanan

1) Pengetahuan kerja

Password

Kata sandi (Inggris: ***password*** atau ***passphrase***) adalah kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Sistem keamanan akan membandingkan kode-kode yang dimasukkan oleh pengguna (yang terdiri atas nama pengguna/*user name* dan *password*) dengan daftar atau basis data yang disimpan oleh sistem keamanan sistem atau jaringan tersebut (dengan menggunakan metode autentikasi tertentu, seperti halnya kriptografi, *hash* atau lainnya). Jika kode yang dibandingkan cocok, maka sistem keamanan akan mengizinkan akses kepada pengguna tersebut terhadap layanan dan sumber daya yang terdapat di dalam jaringan atau sistem tersebut, sesuai dengan level keamanan yang dimiliki oleh pengguna tersebut. Idealnya, kata kunci merupakan gabungan dari karakter teks alfabet (*A-Z*, *a-z*), angka (*0-9*), tanda baca (*!?,.=-*) atau karakter lainnya yang tidak dapat (atau susah) ditebak oleh para *intruder* sistem atau jaringan. Meskipun begitu, banyak pengguna yang menggunakan kata sandi yang berupa kata-kata yang mudah diingat, seperti halnya yang terdapat dalam kamus, ensiklopedia (seperti nama tokoh, dan lainnya), atau yang mudah ditebak oleh *intruder* sistem.

Gambar 3 Bentuk Umum Membuat *Password* Baru (Elemen Kompetensi 1)

Password harus dibuat dengan memperhatikan beberapa hal berikut ini:

- Setidaknya panjang karakter *password* adalah 7 (tujuh) karakter. Anda juga bisa membuat *password* yang lebih panjang lagi demi keamanan.
- Menggunakan sedikitnya 1 (satu) karakter simbol pada deretan karakter *password* Anda.
- Jika sistem Anda menerapkan *password* history, maka pastikan *password* baru Anda selalu berbeda jauh dengan *password* sebelumnya.
- *Password* Anda jangan sampai mengandung nama atau username.
- Jangan gunakan kata-kata yang umum digunakan pada karaktar *password*. Ini termasuk kata-kata yang digunakan dalam kamus.

Beberapa contoh *password* yang kuat misalnya sebagai berikut.
*. a4$Jhi&]
*. 3k>i%uA
*. O@u#5nQ

*Password s*ebenarnya merupakan sistem proteksi yang paling lemah dalam sistem komputer. Maka dari itu memilih *password* yang kuat merupakan suatu keharusan. Mengapa demikian*? Tool password cracking* semakin canggih dalam usahanya membongkar *password*, plus juga komputer yang digunakan dalam *password* cracking semakin baik performanya. *Password* yang sebelumnya butuh waktu seminggu untuk di-crack, maka saat ini bisa di-crack hanya dalam beberapa jam saja.

Software untuk meng-*crack password* biasa menggunakan tiga macam pendekatan yaitu: menebak secara pintar (intelligent guessing), serangan kamus (dictionary attack) dan juga otomatisasi yang berusaha mencoba untuk menggunakan kombinasi karakter. Jika diberi waktu yang cukup, maka metode otomatisasi tersebut bisa meng-crack *password* apa saja. Tetapi jika *password* yang digunakan sangat kuat, maka akan membutuhkan waktu yang sangat lama untuk memecahkannya.

Demikian tips singkat mengenai membuat *password* yang baik dan kuat. Semoga bermanfaat bagi Anda semua

2) Ketrampilan kerja

Pengendalian akses (*access control*) menjadi pertimbangan pertama saat seorang profesional Sistem Keamanan Informasi akan membuat program keamanan informasi. Keistimewaan dan variasi mekanisme *access control* baik secara fisik, teknik dan administrasi akan membangun arsitektur keamanan informasi yang praktis untuk melindungi informasi penting dan sensitif yang menjadi aset organisasi.

Privasi (secara individu) adalah salah satu alasan penerapan *access control* dalam organisasi. Saat ini teknologi telah membuat pertukaran informasi menjadi semakin mudah dan semakin luas, sehingga usaha-usaha perlindungan informasi menjadi semakin kompleks dan sulit.

Jenis-jenis pengendalian dalam keamanan informasi

Keamanan secara umum dapat didefinisikan sebagai bebas dari bahaya atau dalam kondisi selamat. Secara spesifik dalam keamanan komputer didefinisikan sebagai perlindungan data dan komputer dalam sistem terhadap pengungkapan, modifikasi, perusakan atau *denial of service* (DoS) oleh pihak yang tidak berhak.

Sistem pengendalian keamanan komputer secara relatif akan menghambat/menghalangi produktifitas. Untuk itu penerapan keamanan harus selalu dikompromikan secara praktis baik sistem, operasional dan administratif dengan produktifitas organisasi.

A. Pengendalian secara fisik

Keamanan secara fisik (dalam lingkup keamanan informasi) adalah penggunaan kunci, penjagaan, sistem tanda pengenal, alarm dan hal-hal semacam itu yang digunakan untuk pengendalian akses komputer baik alatnya maupun proses dari fasilitas itu. Semua alat-alat dan prosedur tersebut umumnya digunakan untuk mencegah spionase, pencurian, perusakan atau kecelakaan baik akibat bencana alam maupun keteledoran manusia.

1. Pencegahan dalam pengendalian secara fisik

Pencegahan yang dimaksud disini adalah usaha mencegah pihak-pihak yang tidak berhak agar tidak memasuki / menggunakan sumberdaya komputer dan juga melindunginya dari bahaya bencana alam. Hal-hal yang termasuk kategori pencegahan ini adalah :

- ***Back-up*** **file/dokumentasi** : yaitu untuk mencegah agar bila terjadi kecelakaan terhadap sistem komputer, file/dokumen penting tetap ada. Dokumen *back-up* ini sebaiknya disimpan ditempat yang berjauhan dan dengan perlakuan keamanan yang setara dengan dokumen aktifnya.

- **Pemagaran** : yaitu untuk membatasi agar hanya orang-orang yang berhak saja yang dapat memasuki sistem. Termasuk dalam sistem pemagaran adalah CCTV, alarm, anjing penjaga dan pagar.

- **Penjaga keamanan** : pada intinya hampir sama dengan pemagaran namun dengan keunggulan dapat melihat hal-hal yang berkenaan dengan bawaan personel yang akan memasuki area sistem. Agar lebih efektif perlu ditunjang dengan alat-alat elektronik seperti detektor.

- **Sistem tanda pengenal** : yaitu untuk mengenali bahwa orang tersebut adalah pihak yang memang diberikan akses tertentu.

- **Sistem pintu ganda** : biasanya digunakan untuk membedakan level keamanan dalam sebuah sistem. Umumnya pintu 1 adalah area aman dan pintu 2 adalah area terbatas.

- **Kunci** : yang dimaksud adalah kunci (yang terbuat dari) metal dan kunci kriptografi.

- ***Back-up*** **power** : yaitu untuk memastikan tidak ada pemutusan power/listrik secara mendadak yang akan mengakibatkan kerusakan pada sistem. *Back-up* power biasanya berupa baterai cadangan atau generator diesel. Perangkat yang paling populer adalah ups (*uninterruptible power supply*).

- ***Access Control*** **biometrik** : fungsinya hampir sama dengan sistem tanda pengenal, namun menjadi lebih baik karena biometrik menempel pada tubuh, sehingga kecil kemungkinannya untuk hilang atau terlupakan. *Access control* biometrik ini sangat baik digunakan untuk level keamanan tinggi namun dengan pemakaian akses yang jarang.

- **Pemilihan lokasi** : adalah faktor yang sangat penting untuk menghindari resiko yang mungkin timbul akibat bencana banjir, kebakaran, radiasi gelombang elektromagnetik atau yang lainnya.

- **Pemadam kebakaran** : kebakaran akan merusak sistem. Selain lokasi sistem harus jauh dari tempat yang menjadi pemicu kebakaran, material yang digunakan pun sebaiknya yang tidak mudah terbakar. Alat pemadam kebakaran perlu diletakkan ditempat yang tepat dan mudah dijangkau dengan bahan yang baik, sebab bahan pemadam yang buruk akan merusak sistem bagaikan api itu sendiri.

2. Pendeteksian dalam pengendalian secara fisik

Pendeteksian sebagai pengendalian secara fisik merupakan perlindungan atas pelanggaran yang telah terlanjur terjadi. Yang termasuk dalam pendeteksian ini adalah :

- **Detektor gerak** : ruang server komputer umumnya tidak dipakai sebagai lalu-lintas aktifitas manusia, sehingga pemasangan alat deteksi gerak akan sangat berguna untuk mencegah penyusupan.

- **Detektor asap dan api** : bila diletakkan ditempat yang tepat akan sangat berguna sebagai alat pemberitahu yang tercepat bila terjadi kebakaran.

- **CCTV (*Closed-Circuit Television*)** : digunakan untuk memantau kawasan dimana sistem berada/diletakkan.

- **Sensor dan alarm** : digunakan untuk mendeteksi kemungkinan terjadinya penyusupan ke dalam lingkungan dimana sistem berada.

B. Pengendalian secara teknis

Pengamanan secara teknis ini meliputi penggunaan penjaga keamanan, yang mana termasuk didalamnya adalah hardware komputer, sistem operasi dan *software* aplikasi, komunikasi serta peralatan lain yang berhubungan. Pengendalian teknis ini dikenal pula sebagai pengendalian logika.

1. Pencegahan dalam pengendalian secara teknis

Pencegahan secara teknis digunakan untuk mencegah pihak yang tidak berhak baik orang maupun program untuk mengakses sumber daya komputer. Yang termasuk jenis pencegahan ini adalah :

- ***Software Access Control*** : digunakan untuk mengendalikan pertukaran data dan program antar *user*. Biasanya diimplementasikan dalam bentuk daftar *access control* yang mendefinisikan hak akses setiap *user*.

- ***Software* Antivirus** : virus merupakan program yang mewabah dalam komputer serta dapat merusak sistem dan data yang pada akhirnya menghambat produktifitas. Virus baru bermunculan dengan cepat, sehingga pemasangan *software* antivirus yang selalu *up-date* dan selalu aktif dalam komputer merupakan suatu keharusan.

- **Sistem pengendalian pustaka** : mengharuskan semua perubahan program produksi diimplementasikan oleh personel pengendali pustaka ini, hal ini untuk menghindari pihak yang tidak berhak melakukan perubahan.

- ***Password*** : digunakan untuk membuktikan bahwa pengguna atau pemilik ID adalah orang yang memang memiliki hak akses tertentu terhadap sistem.

- ***Smartcard*** : umumnya berbentuk seperti kartu kredit dan dilengkapi chip yang telah diprogram. Informasi didalamnya dapat dibaca di tempat-tempat yang disediakan untuk itu yang dapat mengidentifikasikan hak-hak user. Dalam penggunaannya biasanya dikombinasikan dengan pengendalian akses lainnya seperti password, biometrik, atau ID.

- **Penyandian** : dapat didefinisikan sebagai proses merubah data yang dapat dibaca (*plain-text*) menjadi data yang tidak terbaca (*cipher-text*) oleh algoritma kriptografi.

- **Pengendalian akses *dial-up* dan sistem *call-back*** : digunakan untuk memastikan bahwa hanya pihak yang berhak saja yang dapat melakukan *dial-up* terhadap sistem. Saat ini pengendalian akses *dial-up* yang terbaik menggunakan mikrokomputer untuk menangkap sebuah *call*, memferifikasi identitasnya dan meneruskan *call* pada hak akses sumber daya dalam sistem yang diminta.

Sebelumnya sistem *call-back* menangkap *caller* yang melakukan *dial-up*, memferifikasi otoritasnya, dan kemudian melakukan *call-back* untuk mendapatkan nomor registrasinya.

2. Pendeteksian dalam pengendalian teknis

Memberikan peringatan tentang adanya pelanggaran atau usaha pelanggaran. Yang termasuk pendeteksian ini adalah :

- **Audit trail** : yaitu sistem yang mencatat semua aktifitas dalam sistem. Secara periodik catatan tersebut dilaporkan kepada Administratur keamanan informasi dan database untuk mengidentifikasi dan menyelidiki akses ilegal yang masuk, baik yang berhasil ataupun tidak.

- **Sistem pendeteksi gangguan (*Intrusion Detection System* – IDS)** : akan melacak user yang mengakses kedalam sistem untuk menentukan apakah aktivitasnya diijinkan dan/atau sesuai dengan ijin yang dipunyai. Bila tidak, maka sistem akan memberitahukan Administratur untuk melakukan tindakan.

C. Pengendalian secara Administratif

Administratif atau personel keamanan terdiri dari pembatasan manajemen, prosedur operasional, prosedur pertanggung jawaban, dan pengendalian administratif tambahan untuk menyediakan tingkat perlindungan yang memadai pada sumber daya komputer.

Pengendalian administratif termasuk juga prosedur untuk menyakinkan bahwa semua personel yang mendapatkan akses pada sumber daya komputer, mendapatkan otorisasi dan *security clearance* yang tepat.

1. Pencegahan dalam pengendalian administratif

Pencegahan yang dimaksud disini adalah teknik yang sangat personal untuk melatih kebiasaan orang-orang untuk menjaga kerahasiaan, integritas dan ketersediaan data dan program. Yang termasuk dalam pencegahan ini adalah :

- **Kesadaran keamanan informasi dan pelatihan teknis** : pelatihan untuk menanamkan kesadaran keamanan informasi adalah suatu langkah pencegahan dengan membuat *user* mengerti keuntungan menerapkan keamanan informasi tersebut. Sehingga diharapkan *user* dapat menciptakan iklim yang mendukung.

Pelatihan teknis kepada *user* dapat menolong untuk mencegah terjadinya masalah-masalah keamanan yang biasanya terjadi akibat kesalahan dan kelalaian *user*, misalnya *back-up* dan virus; serta memberikan pemahaman/pelatihan mengenai keadaan darurat, agar *user* dapat mengambil tindakan tepat saat terjadi bencana.

- **Pemisahan/pembagian tugas** : yang dimaksud adalah *user* yang berbeda mendapatkan bertanggung jawab yang berbeda atas tugas-tugas yang berbeda yang merupakan bagian dari keseluruhan proses. Hal ini dilakukan untuk menghindari seorang user menguasai seluruh proses yang membuka peluang bagi kolusi dan manipulasi.

- **Prosedur rekruitmen dan pemberhentian karyawan TI** : prosedur rekruitmen yang tepat akan mencegah organisasi mempekerjakan orang yang berpotensi merusak sistem. Prosedur pemberhentian karyawan TI perlu dibuat dengan cermat agar aset/sumber daya organisasi tidak ikut terbawa keluar, dengan cara menarik seluruh kewenangan atas akses sistem informasi yang dimiliki, misalnya menghapus *password* log-on ID atau mengganti semua kunci aksesnya.

- **Prosedur dan kebijakan keamanan** : merupakan kunci pembentukan program keamanan informasi yang efektif. Kebijakan dan prosedur ini mencakup penggunaan sumber daya komputer, penentuan informasi sensitif, pemindahan sumber daya komputer, pengendalian alat-alat komputer dan media, pembuangan data sensitif yang sudah tidak berguna dan pelaporan keamanan terhadap data dan komputer. Kebijakan dan prosedur ini harus merupakan refleksi dari kebijakan umum organisasi dalam upaya melindungi informasi dan sumber daya komputer.

- **Pengawasan** : harus sejalan dengan kebijakan dan prosedur yang telah ditetapkan oleh organisasi, terutama pada sumber daya organisasi yang sensitif dan rentan terhadap penyalahgunaan wewenang.

- **Perencanaan keadaan darurat dan pemulihan dari bencana** : adalah sebuah dokumen yang berisi prosedur untuk menghadapi keadaan darurat, *back-up* operasional, dan pemulihan instalasi komputer baik sebagian atau seluruhnya yang rusak akibat bencana. Yang paling penting dalam perencanaan ini adalah membuat instalasi komputer bekerja normal kembali dalam waktu yang sesingkat-singkatnya.

- **Registrasi** : *user* perlu melakukan registrasi untuk mendapatkan akses komputer dalam organisasi dan *user* harus bertanggung jawab atas semua sember daya komputer yang digunakannya.

2. Pendeteksian dalam pengendalian administratif

Pendeteksian ini digunakan untuk menentukan seberapa baik prosedur dan kebijakan keamanan dilakukan. Yang termasuk dalam pendeteksian ini adalah :

- **Evaluasi dan audit keamanan** : adalah untuk membantu manajemen agar dapat dengan cepat mengambil tindakan jika terdapat hal-hal yang melenceng dari garis kebijakan dan prosedur yang telah ditetapkan. Evaluasi dan audit ini sebaiknya dilakukan secara periodik.

- **Rotasi tugas dan cuti karyawan TI** : adalah untuk mencegah terjadinya hal-hal yang merugikan sistem seperti membuat kesalahan atau merusak sistem akibat kejenuhan.

- **Penyelidikan** : digunakan untuk mencari potensi resiko atas kinerja sistem dan juga digunakan untuk menyeleksi karyawan TI agar dapat ditempatkan pada posisi yang tepat. Hasil penyelidikan dapat digunakan juga untuk memberikan security clearance atas karyawan dan aset organisasi.

3) Sikap kerja

Sikap kerja ditunjukkan ketika berada dalam lingkungan kerja, yaitu :
1. memperoleh kebutuhan klien berdasarkan petunjuk organisasi
2. memberikan *password* akses ke klien
3. Membuat dokumetasi dan akses keamanan untuk klien
4. mencatat hak akses keamanan demi integritas pemeliharaan sistem.

2. Mencatat lisensi perangkat lunak

1) Pengetahuan kerja

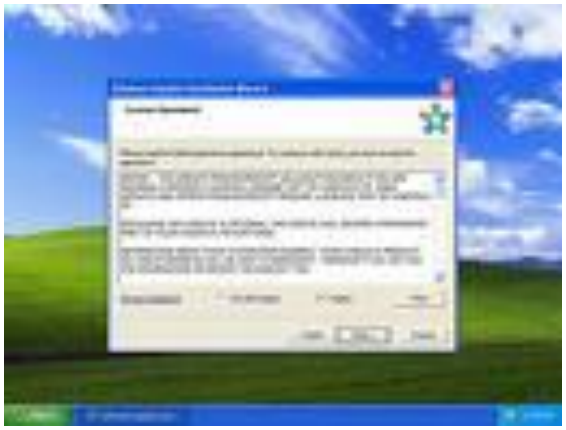
- **Lisensi Perangkat Lunak Bebas**

Sebuah **lisensi perangkat lunak bebas** adalah lisensi perangkat lunak yang mengizinkan pengguna untuk memodifikasi dan mendistribusikan ulang perangkat lunak yang dimaksud. Lisensi ini berlawanan dengan lisensi dari perangkat lunak tak bebas yang melarang pendistribusian ulang atau rekayasa terbalik dari suatu perangkat lunak yang berakibat pada pelanggaran hak cipta.

2) Ketrampilan kerja

Tidak ada catatan lisensi perangkat lunak bebas yang pertama kali digunakan, tetapi perangkat lunak yang diketahui menggunakan lisensi perangkat lunak bebas antara lain adalah TeX dan X11. Pada pertengahan 1980-an, proyek GNU mengeluarkan lisensi-lisensi perangkat lunak bebas yang terpisah untuk masing-masing paket perangkat lunaknya. Kesemuanya digantikan pada 1989 dengan versi satu dari Lisensi Publik Umum GNU (*GNU General Public License* disingkat GPL). Versi 2 dari GPL yang dirilis pada 1991 kemudian menjadi lisensi perangkat lunak bebas yang paling banyak digunakan.

Pada pertengahan hingga akhir 1990-an, muncul sebuah trend baru dimana perusahaan dan proyek baru menulis lisensi baru. Gerakan yang mengakibatkan bermunculannya lisensi-lisensi baru ini berujung kepada masalah komplesitas dan ketidakkompatibilitas. Trend ini akhirnya menurun dan berbalik hingga awal 2000-an.



Gambar 4 Contoh Informasi Lisensi Microsoft (Elemen kompetensi 2)

3) Sikap kerja

Sikap kerja ditunjukkan ketika berada dalam lingkungan kerja, yaitu :
1. Perangkat lunak berlisensi diidentifikasi.
2. Jumlah dan pemakai lisensi didokumentasikan.
3. Personal komputer dan jaringan komputer diperiksa dari perangkat lunak yang tidak legal.
4. Perangkat lunak yang tidak legal dilaporkan kepada pegawas.

3. Menjalankan back up sistem

1) Pengetahuan kerja

Backup dapat diartikan sebagai proses membuat salinan data sebagai cadangan saat terjadi kehilangan atau kerusakan data asli. Salinan data yang dibuat disebut dengan "data *backup*". Manfaat dari proses *backup* diantaranya, mengembalikan kondisi suatu sistem komputer yang mengalami kerusakan atau kehilangan data, mengembalikan suatu file yang tanpa sengaja terhapus atau juga rusak.

Media Penyimpan Data (Storage)

Berbicara masalah proses *backup* tidak akan terpisahkan dengan masalah media penyimpanan data (storage). Setiap *backup* dimulai dengan pertimbangan tempat data *backup* akan disimpan. Data *backup* harus disimpan sedemikan hingga dapat teratur dengan baik. Keteraturan tersebut dapat berupa sesederhana catatan kertas dengan daftar cd-cd *backup* dengan isi datanya yang kita miliki atau dapat pula berupa pengaturan canggih dengan index komputer, katalog atau database relasional. Perbedaaan dalam penggunaan model penyimpanan data akan memberi manfaat yang berbeda. Pengambilan manfaat ini berkaitan erat dengan skema rotasi *backup* yang digunankan.

Pemilihan media penyimpanan data *backup* menjadi pertimbangan yang sangat penting dalam proses *backup*. Ada banyak tipe media penyimpanan yang dapat dipilih dengan kelebihan dan kekurangannya masing-masing.

Tape Magnetic

*Tape magne*tic mirip dengan kaset audio atau kaset video pita yang menyimpan data dalam pita megnet panjang yang berputar dari titik awal hingga titik akhir.

Hardisk

Keunggulan utama dari *hardisk* adalah waktu akses yang cepat, variasi kapasitas yang luas dan kemudahan penggunaan.

Optical Disk

CD dan DVD yang dapat direkam adalah dua pilihan yang ada dalam kategori ini. Namun, dengan semakin murahnya drive DVD dengan kapasitas yang cukup besar, pemilihan DVD sebagai media *backup* lebih menjanjikan daripada CD. Tentunya CD pun masih bisa digunakan untuk proses *backup* kelompok data yang lebih kecil.

Floppy Disk

Media pada masanya sudah mencukupi tuntutan penyimpanan data. Tapi, sekarang sudah tidak ada lagi alasan untuk menggunakan media ini, apalagi untuk keperluan *backup*. Dengan semakin besarnya file-file yang dimiliki orang seperti video, musik, hingga data sistem, merupakan hal yang tidak masuk akal menjadikan floppy disk sebagai pilihan.

Solid State Storage

Yang masuk dalam kelompok media ini ada banyak, diantaranya flash memory, thumb drives, compact flash, memory stick, secure digital cards, multi media card, dan seterusnya. Portabilitas adalah keunggulan sekaligus kelemahan media *backup* ini. Dengan portabilitasnya, data pada media ini sangat mudah dipindahkan termasuk berpindah ke tangan yang tidak seharusnya.

Remote Backup Services

Media ini tidak berupa benda fisik yang nyata, namun berupa service atau layanan. Biasanya perusahaan penyedia jasa ini menyewakan ruangan penyimpanan data yang proses akses dan pengaturan data *backup* dilakukan melalui internet. Untuk segi keamanan, metode ini sangat menjanjikan. Tapi, untuk kondisi Indonesia dengan kualitas koneksi internetnya yang masih mengecewakan, masih memerlukan waktu untuk implementasi luas metode *backup* ini.

2) <u>Ketrampilan kerja</u>

Manipulasi data

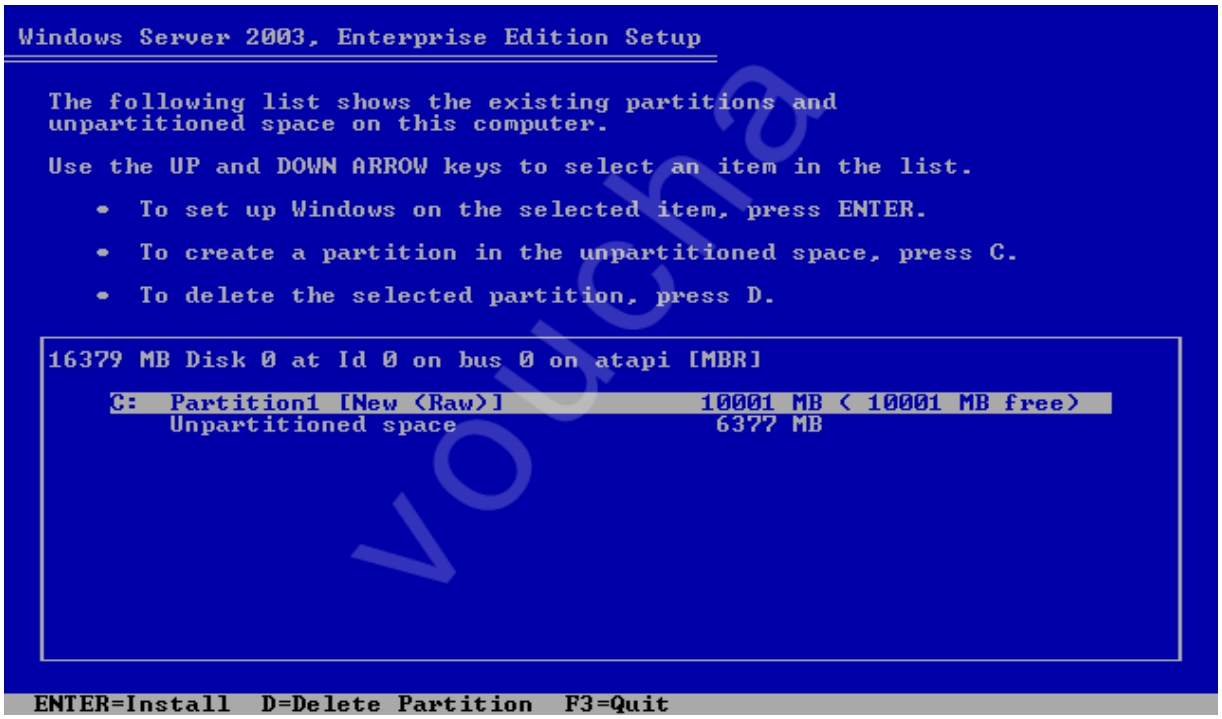
Dalam proses *backup*, data dapat disimpan dalam format apa adanya atau dapat pula dilakukan manipulasi untuk optimasi *backup* itu sendiri. Dua proses manipulasi yang biasa dilakukan adalah kompresi dan enkripsi. Kompresi memampatkan ukuran file untuk menghemat ruangan penyimpanan data. Enkripsi menjadi isu penting saat berkaitan dengan *backup* data yang bersifat penting dan rahasia. Enkripsi menyimpan data bukan dalam format asli namun telah disembunyikan dalam bentuk sandi-sandi algoritma tertentu. Dengan enkripsi hanya orang yang memiliki akses kunci enkripsi yang dapat membaca data sesungguhnya. Dengan mengimplementasikan pengamanan data *backup* melalui enkripsi akan memperlambat proses *backup* itu sendiri. Namun, nilainya tentunya sebanding bila data yang di*backup* merupakan data yang sangat penting.

Setiap pengguna komputer pastinya tidak dapat lari dengan berbagai masalah, baik masalah kecil ataupun besar. Masalah tersebut mungkin berbagai macam *alert warning,* larangan, atau *error* karena *bug.* Selain itu, ada pula kemungkinan masalah yang berasal dari modem, *vga card, sound card, CD player,* dll atau mungkin juga dari sistem operasi yang Anda pakai sendiri. Dari sejumlah masalah tersebut, ada beberapa masalah yang sangat lebih memusingkan lagi yaitu karena ancaman *hacker, spam, virus,* dan *worm*. Masalah –masalah ini sangat mengganggu bagi para pejabat, pekerja, ataupun para *user* untuk PC di rumah.
Seiring dengan perkembangan kemajuan teknologi yang semakin canggih, kini kita bisa memanfaatkan internet dengan kecepatan yang sudah cukup tinggi dan kapasitas *download* yang semakin besar. Namun perkembangan teknologi yang semakin canggih ini terkadang seringkali disalahgunakan oleh segelintir orang. Banyak diantara mereka yang sangat aktif menyebarkan virus, *spyware*, a*dware*, maupun *riskware*.

Komputer yang telah terjangkit virus, *spyware*, a*dware*, maupun *riskware* seperti diatas secara otomatis akan mengalami masalah-masalah selanjutnya (kelumpuhan pada sistem operasi, program, aplikasi, data dan kerusakan *hardware)*. Hal ini tentu saja sangat mengganggu dan merugikan data. Karena seringkali hal ini menyebabkan data-data yang menjadi hilang atau rusak. Ada alternatif yang bisa dilakukan untuk menghilangkan virus, *spyware*, a*dware*, maupun *riskware* yaitu dengan cara memformat data dan menginstal ulang sistem operasi seperti Windows lagi. Hal ini tentu saja akan menghilangkan semua data-data yang telah ada. Hal ini menyebabkan kerugian pada biaya dan waktu. Oleh karena itulah, kita harus melakukan sistem *backup*. *Back up* disini meliputi *backup* untuk sistem operasi dan *backup* data.

Untuk melakukan proses *backup* ini, Anda perlu mempunyai 2 partisi. Sebaiknya 2 partisi ini merupakan jenis yang sana, dan sebaiknya jenisnya NTFS. Hal ini dikarenakan karena jenis NTFS bisa menampung hardware (hard disk) yang berkapasitas besar untuk datanya.

Berikut ini contoh proses partisi. Dan partisi yang sedang aktif adalah C yang digunakan untuk menyimpan windows.



Gambar 5 Partisi untuk Hard Disk (Elemen kompetensi 3)

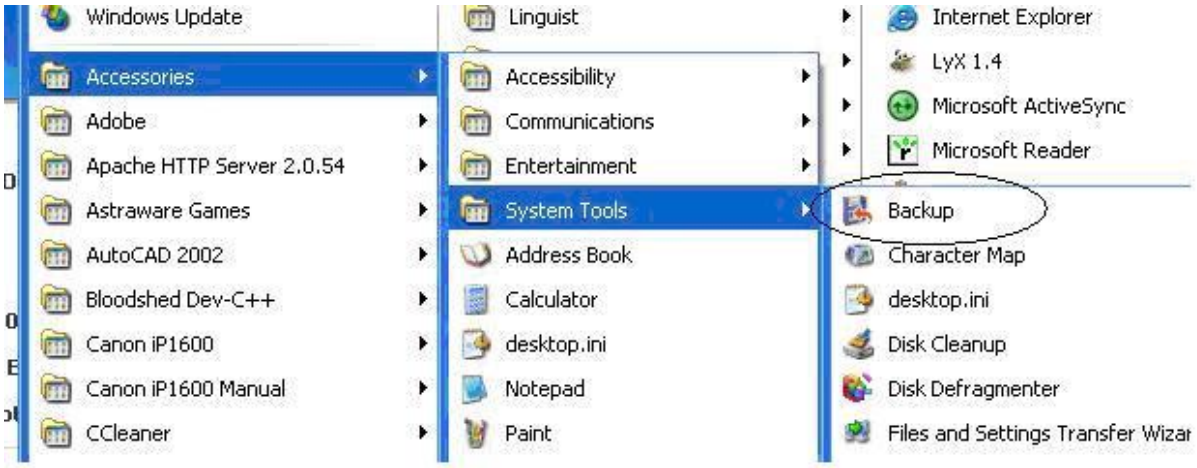
Dalam contoh diatas, partisi akan dilakukan untuk C dan bisa menambah partisi untuk D. Partisi C berfungsi untuk menyimpan data dan file –file yang berhubungan dengan Windows atau sistem operasi. Biasanya partisi C diberi label WinXP sebagai pengingat partisi C merupakan *backup* data Windows atau sistem operasi yang digunakan. Sedangkan partisi-partisi yang lain bisa diberi nama sesuai kebutuhan, misal Data, Music, dan lain-lain. Sehingga jika dilakukan format windows, data tidak akan hilang. Karena format hanya dilakukan pada C saja. Selanjutnya folder C hanya dilakukan untuk penginstalan berbagai aplikasi tambahan seperti Adobe Photoshop, ACD See, Microsoft Office, dan lain-lain.

Restore dan *recovery* adalah proses penting setelah *backup*. *Backup* akan menjadi sia-sia bila proses pengembalian dan perbaikan data sistem sulit dilakukan. Untuk mencapai tujuan ini ada beberapa pendekatan yang harus diperhatikan, yaitu proses *backup* harus dilakukan

dengan aturan yang jelas, hindari mem*backup* dengan sembarangan dengan tidak terstruktur. Selain itu, banyak *software* yang ada di pasaran (baik gratis maupun berbayar) yang memberikan kemudahan *backup* data. Dengan *software* yang sama biasanya proses *restore* dan *recovery* data akan lebih mudah dilakukan. Beberapa *software backup* memiliki fasilitas penjadwalan otomatis proses *backup*. Fitur ini sangat bermanfaat untuk digunakan karena menjamin proses *backup* selalu dilakukan dengan teratur.

Software backup biasanya telah menjadi fasilitas bawaaan beberapa sistem operasi. Misal Windows XP memiliki Nt*backup*.exe, *software* bawaan Windows XP. Dalam beberapa kasus, penggunaan Nt*backup*.exe sudah mencukupi untuk *backup* data.

Nt*backup*.exe dapat diakses dari menu run, ketik: Nt*backup*.exe. Dapat juga diakses dari start menu à accesesoris à System Tools à *Backup*. Seperti *software-software* windows lain, Nt*backup*.exe sangat mudah digunakan, apalagi dengan fasilitas wizard yang disertakan. Proses restore data pun sama mudahnya. Tinggal ikuti saja langkah-langkah yang diberikan.



Gambar 6 Pilihan Aplikasi untuk Restore Data dari Windows
(Elemen Kompetensi 3)

Selain Nt*backup*.exe, banyak *software* lain yang dapat digunakan untuk *backup* data. Salah satunya yang cukup populer adalah Nero. Fungsi utama Nero sebagai *software* burning cd sangat mempermudah keperluan *backup*.

Gambar 7 *Backup* Data dari Nero (Elemen kompetensi 3)

3) Sikap kerja

Sikap kerja ditunjukkan ketika men

1. Prosedur *backup* ditentukan berdasarkan petunjuk organisasi.
2. *Back up* dilaksananan sesuai periode berdasarkan spesifikasi organisasi.
3. *Back up* dicatat sesuai petunjuk organisasi.

4. Memulihkan (restore) sistem dengan menggunakan backup

1) Pengetahuan kerja

Restore dan *recovery Software*

Restore software adalah kasus khusus dari restore data. Penggunaan *software* baik aplikasi maupun sistem operasi biasa tidak akan berjalan sempurna selamanya. Ada masanya bila *software* sudah terlalu lama diinstal dan digunakan akan mulai terjadi konflik librari, kerusakan file, hilang file yang berujung *software* tidak dapat digunakan lagi. Bila masa ini telah tiba ada beberapa hal yang dapat dilakukan. Pertama untuk kasus recovery *software* aplikasi.

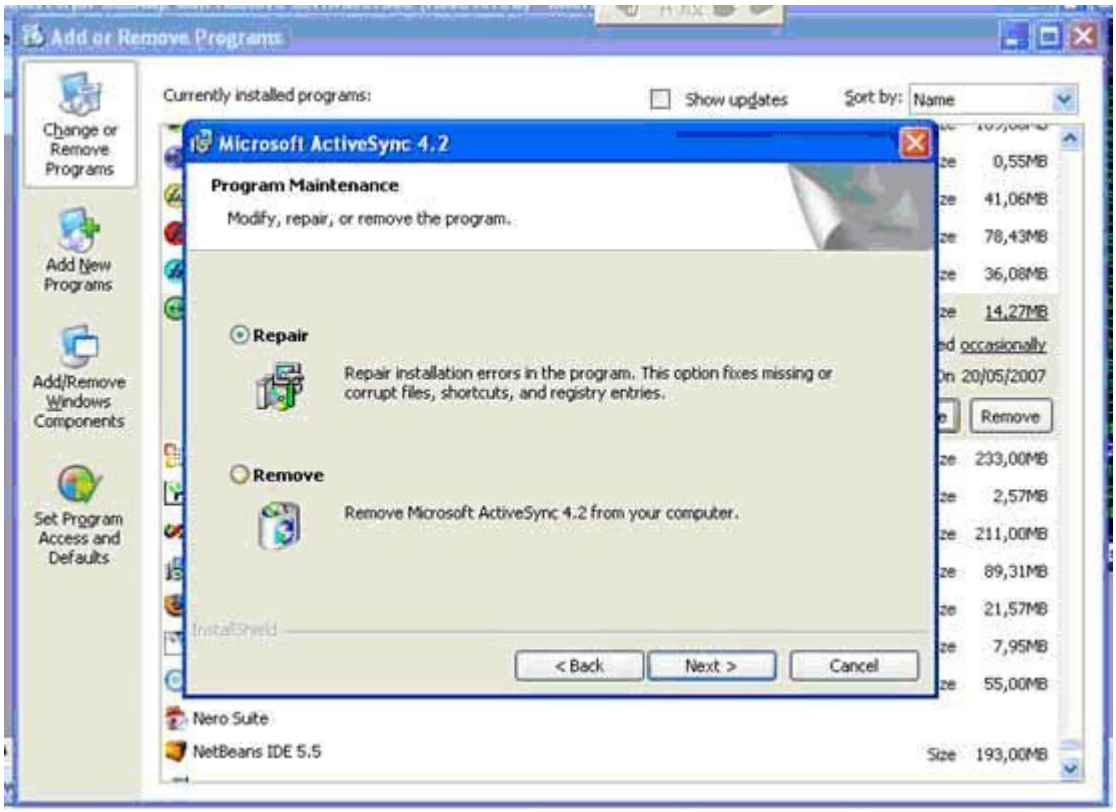
2) Ketrampilan kerja

Beberapa *software* aplikasi memiliki fitur *repair* dalam menu add/remove program. Fitur ini dapat dimanfaatkan bila *software* terinstal sudah mulai tidak berfungsi dengan benar. Dalam kasus terburuk, bila repair belum memperbaiki fungsi *software* yang rusak, proses restore dapat dilakukan dengan menginstal ulang *software* bersangkutan. Tentunya sebelum proses

dilakukan, file-file tersimpan yang berkaitan dengan *software* tersebut harus di*backup* terlebih dulu.

Restore software adalah kasus khusus dari restore data. Penggunaan *software* baik aplikasi maupun sistem operasi biasa tidak akan berjalan sempurna selamanya. Ada masanya bila *software* sudah terlalu lama diinstal dan digunakan akan mulai terjadi konflik librari, kerusakan file, hilang file yang berujung *software* tidak dapat digunakan lagi. Bila masa ini telah tiba ada beberapa hal yang dapat dilakukan. Pertama untuk kasus *recovery software* aplikasi.

Beberapa *software* aplikasi memiliki fitur *repair* dalam menu add/remove program. Fitur ini dapat dimanfaatkan bila *software* terinstal sudah mulai tidak berfungsi dengan benar. Dalam kasus terburuk, bila repair belum memperbaiki fungsi *software* yang rusak, proses restore dapat dilakukan dengan menginstal ulang *software* bersangkutan. Tentunya sebelum proses dilakukan, file-file tersimpan yang berkaitan dengan *software* tersebut harus di*backup* terlebih dulu.

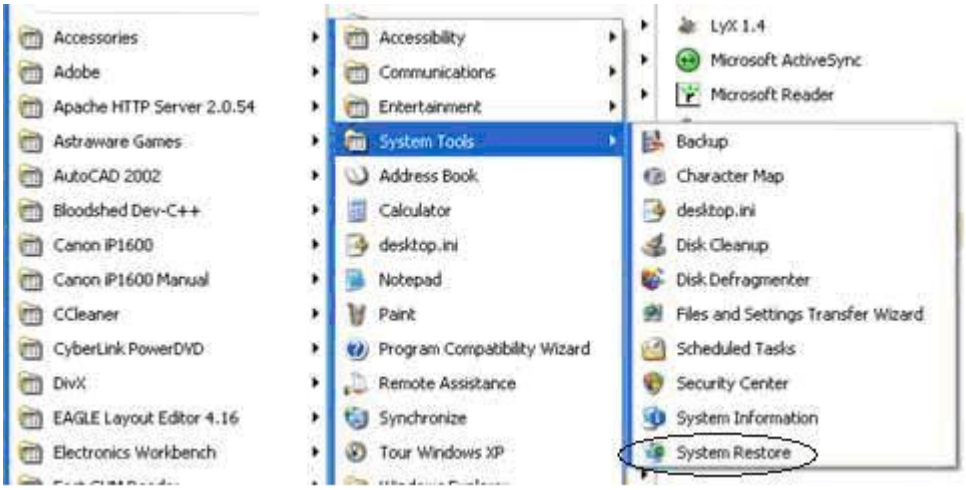


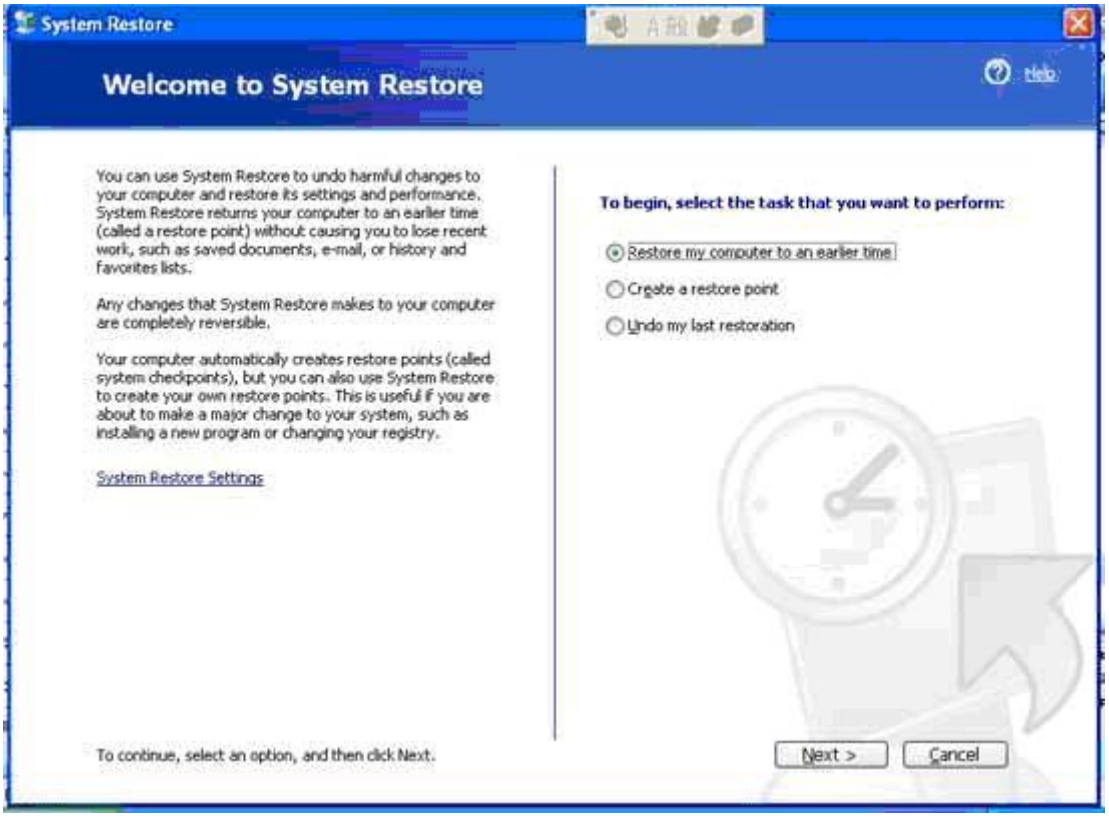
Gambar 8 fitur repair dalam menu *add/remove program*

Kasus recovery *software* kedua adalah untuk Sistem Operasi (SO). Berbeda dengan recovery *software* aplikasi, sistem operasi bersifat lebih kompleks dan melibatkan sistem secara keseluruhan. System Restore adalah tool pada Windows XP yang berfungsi untuk menanggulangi kerusakan SO. Cara kerja System Restore adalah memonitor storage SO dan perubahan-perubahan yang terjadi didalamnya secara sistem. Pada titik-titik tertentu System Restore membuat semacam checkpoint yang dibuat secara otomatis dan bisa juga ditetapkan oleh user. Pada checkpoint tersebut System Restore membuat semacam

penunjuk. Saat terjadi kerusakan SO, pengguna dapat menggunakan System Restore untuk me-restore *software* dengan

cara kembali ke titik checkpoint terdahulu saat masalah tersebut belum terjadi. Sama seperti Nt*backup*.exe, penggunaan *System Restore* sangat mudah diikuti.





Gambar 9 penggunaan *System Restore*

3) Sikap kerja

Sikap kerja ditunjukkan saat beraktivitas di ruang kerja yaitu :

1. Prosedur me-*restore* ditetapkan berdasarkan petunjuk organisasi.
2. *Back up* sistem di-*restore* sesuai dengan permintaan pihak yang berwenang dan dijalankan di bawah instruksi pengawas.
3. *Restore* dicatat sesuai dengan petunjuk organisasi.

Mendokumentasikan akses keamanan

1) Pengetahuan kerja

Pendahuluan

Keamanan, merupakan satu kebutuhan pokok hampir di semua bidang terlebih lagi di bidang IT sampai saat ini. Tidak heran banyak instansi dan perusahaan berani membayar harga mahal hanya untuk keamanan. Hal ini dikarenakan kekhawatiran pada kejahatan penyusupan dan penyadapan informasi tentu saja melalui berkas yang disimpan pada media penyimpanan.

Keamanan dalam tulisan ini dititik beratkan pada keamanan berkas, yaitu menjaga keutuhan, kerahasiaan supaya tidak dapat diketahui oleh pihak-pihak yang tidak diinginkan (penyusup). Berbagai metode dilakukan, baik dari sisi sistem operasi yang berjalan, maupun dari isi yang dilakukan dengan enkripsi dan penggunaan user beserta hak akses yang berbeda pada suatu sistem database.

Keamanan berkas tentu saja tidak dapat lepas dari peranan sistem operasi yang menjadi dasar pengorganisasian berkas itu. Sehingga disini juga akan diurai tinjauan mekanisme keamanan dari beberapa sistem operasi yang sering digunakan.

Dari sisi sistem operasi dapat dilihat ciri khusus penerapan kemanan file pada sistem operasi multi user misalnya : Linux dan keluarga Unix, Windows 2000/NT/XP. Dan akan dibandingkan dengan sistem operasi single user yaitu Windows 95/98/98SE maupun generasi sebelumnya yaitu DOS.

Sedangkan pada pengamanan file dengan cara enkripsi adalah menerapkan algoritma enkripsi yang kunci dekripsinya hanya dipegang oleh orang-orang yang berhak saja. Pada database multiuser biasanya diterapkan hak akses dan kewenangan pada database itu. Misalnya Interbase, MySQL, MSSQL, Oracle, Informix dan lain-lain.

Kemananan juga tidak hanya pada level akses baca saja. Juga meliputi penghapusan file supaya tidak meninggakan jejak pada saat berkas itu dihapus. Misal dalam Sistem Operasi keluarga Microsoft Windows yaitu dengan SecureDelete, Norton Utilities dan lain-lainnya.

Keamanan Berkas melalui Sistem Operasi

Keamanan berkas yang diserahkan pada sisem operasi biasanya ada pada sistem operasi multiuser. Banyak pengguna, sehingga data masing user harus dijaga supaya user lain tidak boleh membaca, menghapus, mengeksekusi dan lain sebagainya. Hal ini digunakan untuk menjamin privasi dan keamanan/kerahasiaan data user. Akan diurai sedikit pada beberapa sistem operasi yang terkenal yaitu : Linux dan Microsoft Windows.

LINUX dan Keluarga Unix

Di sini manajemen file diberi *permision*/hak akses bagi *owner, group* dan *other*. Hak akses itu antara lain : ***r****ead,* ***w****rite,* ***ex****ecute*. Tambahan berupa **s**uid/**g**id dan **t**emporari. Juga ada tambahan attribute yaitu *immutable* yang membuat file tidak bisa dihapus, maupun diubah. Contoh list direktori milik mastris :

```
[mastris@webstudent mastris]$ ls -al
total 4048
drwx--x--x   12 mastris  mastris      4096 Apr 28 12:17 .
drwxr-xr-x    5 root     root         4096 Apr 26 23:52 ..
drwx------    4 joe      student      4096 Mar  6 21:39 install
drwxr-xr-x   11 mastris  mastris      4096 Apr 26 23:26 psybnc
-rw-r--r--    1 mastris  mastris    643257 Oct 12  2002 psybnc.tar.gz
-rw-------    1 mastris  mastris      4394 Jan 12 15:19 ptrace24.c
drwxrwxr-x    3 mastris  mastris      4096 Apr 26 18:25 public_html
drwxrwxr-x    4 mastris  wheel        4096 Apr 27 06:23 rpm
```

Dapat dilihat pada kolom pertama menunjukkan *permission* dari file/direktori, sedangkan kolom 3 dan 4 menunjukkan siapa pemiliknya dan masuk dalam group mana. Dengan demikian bila di dalam server itu ada user lain misalkan bernama vembri maka vembri tidak dapat mengubah(write) file-file yang ada di direktori home-nya mastris.

Pada bagian yang dicetak tebal, rpm milik mastris dan group wheel, kemudian group wheel diberi akses rwx, yaitu bisa membaca, mengubah isi dan eksekusi.

Dengan adanya pengorganisasian dan penerapan permission semacam ini dalam sistem operasi Linux maka kemanan data dari masing-masing user dapat dijaga. User dapat menentukan sendiri *permision mode*nya sendiri. Jadi tidak sembarang orang dapat melihat, membaca, menghapus, menjalankan ataupun memodifikasinya.

Untuk melakukan pengorganisasian file semacam ini Linux menggunakan tipe file sistem Exended2. Bahkan sekarang file sistem tipe Ext2 ini telah disempurnakan menjadi Ext3.

Windows 2000/NT/XP

Pada sistem operasi ini direkomendasikan menggunakan tipe file sistem NTFS (*New Technologi File System*). Karena NTFS menyediakan fitur EFS (*The Encrypting File System*) yang menjamin keamanan data penggunanya dengan cara dienkripsi. Walaupun media penyimpan dicuri, tetapi data didalamnya tidak dapat dicuri tanpa *password* yang digunakan untuk membukanya. Hal ini tentunya sangat menjamin kerahasiaan data yang benar-benar besifat rahasia.

Jadi masing-masing user dalam penyimpanan datanya ke fisik media penyimpan yang bertipe NTFS adalah dienkrip.

Keterangan lebih lanjut dan seluk beluk NTFS dapat dibaca di : http://www.ntfs.com/.

Windows 95/98/98SE dan DOS

Windows 95/98/98SE dan DOS tidak didesain sebagai sistem operasi multiuser, sehingga jaminan keamanan data masing-masing user sangat rendah. Sehingga nantinya keamanan file dari user dapat dilakukan dengan enkripsi dengan menggunakan *third party sofware* yang akan dijelaskan pada bagian selanjutnya.

Third Party *Software* merupakan *software* tambahan, yang tidak disertakan secara default pada instalasinya.

Di sistem operasi ini tipe file sistem yang digunakan adalah FAT. Merupakan tipe file sistem yang kuno. FAT didesain oleh BillGates pada tahun 1976, merupakan tipe file sederhana. Fitur-fiturnya pun masih sederhana tanpa adanya fasilitas enkripsi, tetapi sederhana dalam pengimplementasiannya dan perhitungan didalamnya. Tipe file sistem ini digunakan pada sistem operasi produk dari Microsoft, tetapi saat ini kebanyakan sudah menggunakan NTFS sebagai file sistemnya.

2) Ketrampilan kerja

Keamanan Berkas dengan Enkripsi dan File ber-*password*

Dengan menyimpan file dengan dienkrip maka resiko pencurian informasi dapat dikurangi. Banyak metode / algoritma yang dapat diterapkan untuk mengenkripsi file yang terkenal misalnya PGP dan masih banyak lagi lainnya. Dengan demikian walaupun berkas dapat dikopi/dicuri tetapi untuk mengetahui informasi didalamnya memerlukan usaha lagi untuk memecahkan kode enkripsi untuk mendapatkan file aslinya. Intinya adalah pengamanan berkas.

PGP terdiri dari dua kunci. Kunci privat dan kunci public. Data yang dienkrip dengan public key dan dapat dibuka dengan private key. Demikian sebaliknya. Hal ini sudah banyak diterapkan pada pengiriman e-mail dengan fasilitas internet.

File yang disimpan di enkrip terlebih dahulu, pada waktu ingin membukanya dilakukan pendekripsian. Juga dapat diterapkan penyertakan permintaan *password* untuk membuka berkas. Misalnya file dokumen dari MSWord dapat diberi *password*, file PDF maupun file-file terkompresi seperti ZIP dan RAR. Sehingga untuk dapat membukanya hanya orang yang mempunyai *password* saja yang dapat melakukannya.

Keamanan Database dengan Manajemen User

Tidak hanya sistem operasi saja yang mempunyai mekanisme pembatasan akses bagi user-usernya. Dalam database multiuser misalnya Intebase, MySQL, MSSQL, Oracle, Informix dan lain-lain, juga diterapkan tingkat kekuasaan suatu user.

Diambil contoh dalam database Interbase, SYSDBA merupakan user yang paling berkuasa di dalam database itu. Dapat menambah, menghapus user maupun modifikasi struktur dan content database itu sendiri. Sedangkan user biasa yang misalnya diberi wewenang SELECT saja maka dia tidak akan bisa INSERT, UPDATE maupun DELETE. Jadi haknya sebatas SELECT saja.

Untuk masuk ke database, user harus melakukan proses login/authentikasi. Setelah masuk, berdasarkan definisi di dalam sistem database itu user ini berprevilege sebagai apa. Sehingga dengan demikian diharapkan user biasa tidak membahayakan sistem database.

2. **Penghapusan Berkas**

Penghapusan dilakukan guna menghilangkan data yang sudah tidak diperlukan lagi. Penghapusan yang aman adalah penghapusan yang benar-benar hilang, tidak dapat dikembalikan lagi. Di dalam sistem operasi Microsoft Windows misalnya,

penghapusan dilakukan dengan mengubah karakter pertama nama file sehingga menunjukkan file itu telah terhapus. Tetapi cara ini merupakan cara yang tidak aman untuk menghapus data, karena masih dapat dikembalikan seperti semula bila fisik medium belum tertimpa oleh data lain.

Hal ini diperlukan juga misalnya komputer kita atau media penyimpanan kita akan diberikan kepada orang lain. Tentu saja yang diberikan berupa fisik barang, bukan berupa data yang ada didalamnya. Sehingga untuk benar-benar menghapus data didalamnya dilakukan metode ini.

Untuk menghapus file yang benar-benar aman adalah dengan cara menimpa fisik medium dengan data nol atau data acak, sehingga file sudah benar-benar musnah dan tidak dapat dikembalikan seperti sedia kala.
Banyak program yang dapat melakukan ini, misalnya SecureDelete, Utiliti dari Norton, sehingga dapat dipastikan tidak ada sisa lagi dari berkas yang dihapus.

3) Sikap kerja

1. Akses keamanan didokumentasikan sesuai petunjuk keamanan.
2. Register akses keamanan dipelihara sesuai petunjuk organisasi.