Komunikasi *wireless* memang tidak tampak mata, namun nyatanya Anda dapat berkomunikasi dengan lawan Anda melalui media ini. Kenalilah istilah dan terminologi di dalamnya untuk dapat lebih memahami penggunaannya.

Hayri

Serba-serbi Wireless

Komunikasi data membutuhkan sebuah media penghantar agar informasi yang ingin disampaikan dapat berjalan ke tujuannya dengan baik. Media komunikasi data bisa berwujud apa saja, selama media tersebut dapat menghantarkan informasi dengan baik tanpa ada cacat-cacat yang berarti. Selama bertahun-tahun hingga saat ini pun, media komunikasi data didominasi oleh media komunikasi kabel. Namun, kini arah trennya sudah mulai bergerak menuju ke jenis media lain yang tidak kalah hebat dan menariknya. Media yang sedang naik daun tersebut adalah media wireless LAN atau yang biasa disingkat WLAN.

Media jenis ini bukanlah media baru dalam dunia komunikasi data, namun perkembangannya yang terus-menerus menuju ke arah yang lebih baik membuatnya semakin disukai oleh masyarakat. Dengan semakin berkembangnya kualitas media ini menghantarkan data, jarak jangkauannya yang semakin jauh, kekebalannya yang semakin tinggi dalam menangani interferensi, dan banyak lagi perkembangan lainnya, membuat pengguna media ini semakin meningkat dari hari-ke hari. Tidak bisa dipungkiri, media ini mungkin akan menguasai dunia komunikasi data beberapa tahun mendatang. Khususnya komunikasi data dalam jaringan lokal (LAN).

Karena semakin meluasnya penggunaan media ini, maka ada baiknya bagi Anda untuk mengenal lebih jauh apa sih sebenarnya teknologi wireless LAN ini. Mungkin WLAN sudah bukan merupakan barang baru lagi, namun seluk-beluknya perlu Anda pahami benar-benar jika ingin menggunakannya dengan nyaman. Apalagi jika Anda ingin menggunakannya dalam skala besar, tidak ada salahnya untuk mengetahui lebih banyak lagi apa *sih* sebenarnya WLAN itu, apa yang ada di dalamnya, dan banyak lagi.

Berikut ini adalah beberapa pertanyaan yang sering muncul di benar Anda mengenai teknologi WLAN ini.

1. Apa Itu Wireless LAN (WLAN)?

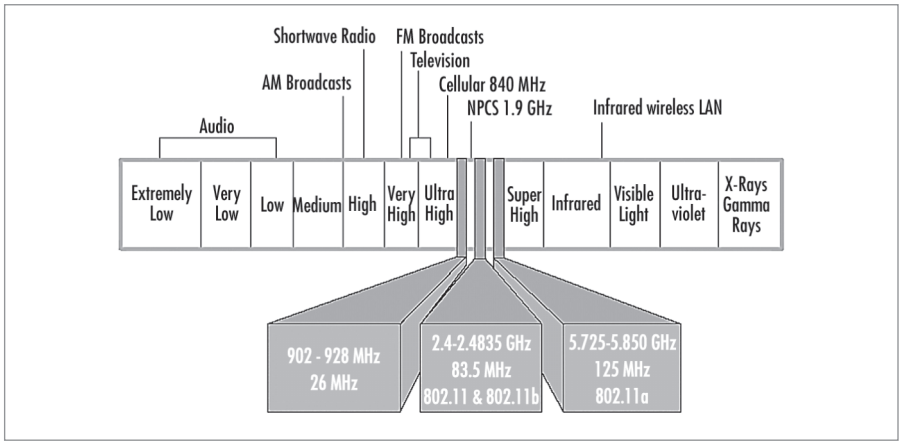
Mungkin bagi sebagian orang istilah ini sudah tidak asing lagi bahkan sudah terkesan basi. Namun, tidak sedikit pula yang lupa atau bahkan belum tahu apa itu WLAN. Sebenarnya WLAN adalah sebuah jaringan lokal (LAN) yang terbentuk dengan menggunakan media perantara sinyal radio frekuensi tinggi, bukan dengan menggunakan kabel. Wireless LAN ini memiliki tingkat fleksibilitas yang lebih tinggi daripada media kabel. Maka dari itu, WLAN sering digunakan sebagai ekstensi dari komunikasi melalui media kabel atau sebagai media alternatif bagi komunikasi melalui kabel.

2. Apa Untungnya Menggunakan WLAN daripada Media Kabel?

Media *wireless* yang tidak kasat mata menawarkan cukup banyak keuntungan bagi penggunanya. Berikut ini adalah beberapa keuntungannya:

- **Meningkatkan produktivitas**

Jaringan WLAN sangat mudah untuk diimplementasikan, sangat rapi dalam hal fisiknya yang dapat meneruskan informasi tanpa seutas kabel pun, sangat fleksibel karena bisa diimplementasikan hampir di semua lokasi dan kapan saja, dan yang menggunakannya pun tidak terikat di satu tempat saja. Dengan semua faktor yang ada ini, para penggunanya tentu dapat melakukan pekerjaan dengan lebih mudah. Akibatnya pekerjaan menjadi lebih cepat dilakukan,



Komunikasi *wireless* sudah dimulai sejak dulu. Hal ini terlihat dari banyaknya frekuensi *range* yang telah dialokasikan untuk berbagai keperluan.

tidak membutuhkan waktu yang lama hanya karena masalah-masalah fisikal jaringan dari PC yang mereka gunakan.

Berdasarkan faktor inilah, wireless LAN tentunya dapat secara tidak langsung meningkatkan produktivitas kerja dari para penggunanya. Cukup banyak faktor penghambat yang ada dalam jaringan kabel dapat dihilangkan jika Anda menggunakan media ini. Meningkatnya produktivitas kerja para karyawannya, tentu akan sangat bermanfaat bagi perusahaan tempat mereka bekerja, bukan?

- **Cepat dan sederhana implementasinya**

Implementasi jaringan WLAN terbilang mudah dan sederhana. Mudah karena Anda hanya perlu memiliki sebuah perangkat penerima dan pemancar untuk membangun sebuah jaringa wireless. Setelah memilikinya, konfigurasi sedikit dan Anda siap menggunakan sebuah jaringan komunikasi data baru di dalam lokasi Anda. Namun, tidak sesederhana itu jika Anda menggunakan media kabel.

- **Fleksibel**

Media *wireless* LAN dapat menghubungkan Anda dengan jaringan pada tempat-tempat yang tidak bisa diwujudkan oleh media kabel. Jadi fleksibilitas media wireless ini benar-benar tinggi karena Anda bisa memasang dan menggunakannya di mana saja dan kapan saja, misalnya di pesta taman, di ruangan *meeting* darurat, dan banyak lagi.

- **Dapat mengurangi biaya investasi**

Wireless LAN sangat cocok bagi Anda yang ingin menghemat biaya yang akan dikeluarkan untuk membangun sebuah jaringan komunikasi data. Tanpa kabel berarti juga tanpa biaya, termasuk biaya kabelnya sendiri, biaya penarikan, biaya perawatan, dan masih banyak lagi. Apalagi jika Anda membangun LAN yang sering berubah-ubah, tentu biaya yang Anda keluarkan akan semakin tinggi jika menggunakan kabel.

- **Skalabilitas**

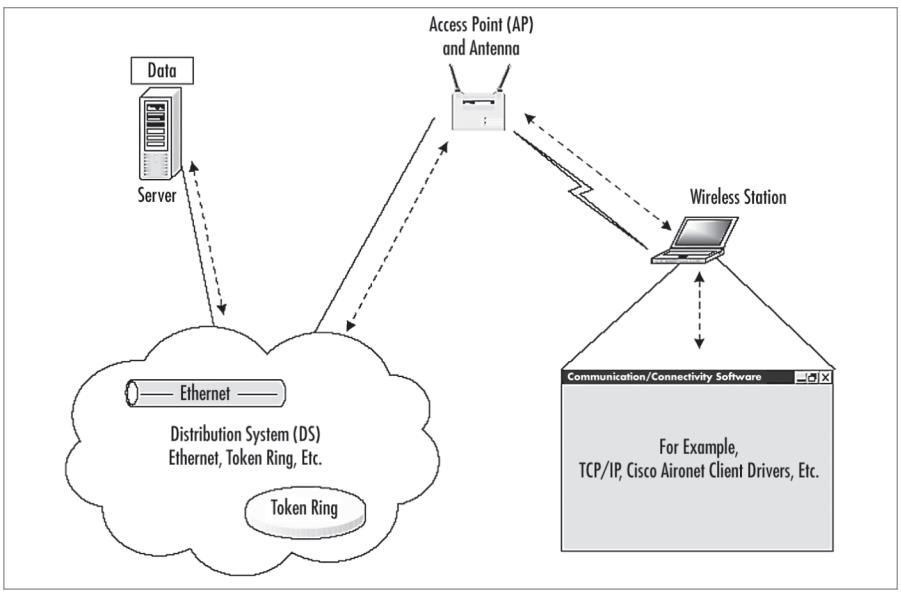
Dengan menggunakan media wireless LAN, ekspansi jaringan dan konfigurasi ulang terhadap sebuah jaringan tidak akan rumit untuk dilakukan seperti halnya dengan jaringan kabel. Di sinilah nilai skalabilitas jaringan WLAN cukup terasa.

3. Apa Maksud dari Istilah 802.11a/b/g?

Istilah ini merupakan sebuah nomor standardisasi dari sistem WLAN yang ada saat ini. Dalam standardisasi ini diatur apa dan bagaimana jaringan WLAN bekerja. Mulai dari teknik modulasi sinyalnya, frekuensi *range*-nya, sampai jenis antena yang cocok digunakan. Masing-masing standar memiliki spesifikasi teknis yang berbeda-beda. Dengan demikian cara kerja, perangkat pendukung, dan performa yang dihasilkan dari setiap standar tersebut berbeda-beda satu sama lain.

Akibat dari kondisi ini, ketiga standar tersebut tidak dapat saling berhubungan satu sama lain. Maksudnya perangkat yang menggunakan standar 802.11a tidak akan dapat bekerja pada AP yang menggunakan standar 802.11b, begitu seterusnya.

Mungkin sebagian besar pengguna jaringan wireless pasti sudah pernah mendengar istilah yang terdiri dari angka dan huruf ini. Memang benar ketika Anda ingin menggunakan jaringan wireless, Anda harus mengetahui lebih dahulu perangkat Anda bekerja di standar yang mana. Karena jika Anda membeli perangkat yang tidak cocok dengan perangkat AP atau perangkat



AP dapat mengubah media apapun menjadi terhubung dengan jaringan *wireless*, semua tergantung pada *interface* yang ada pada AP tersebut.

wireless lainnya, maka Anda tidak mungkin dapat terkoneksi ke jaringan tersebut. Untuk itu, sangat disarankan Anda meneliti dulu perangkat wireless Anda bekerja pada jenis apa.

Saat ini standar yang paling umum digunakan adalah standar 802.11b dan 802.11g. Namun, saat ini tidak jarang juga sebuah perangkat wireless sengaja dibuat dengan memiliki kemampuan bekerja pada ketiga standar tersebut. Jadi satu perangkat dilengkapi dengan tiga spesifikasi yang berbeda. Dengan demikian, Anda tidak akan kesulitan untuk terkoneksi kedalam jaringan wireless dengan standar apapun.

4. Mengapa Standar 802.11b dan g Bekerja Menggunakan Frekuensi 2,4 GHz?

Kedua standar tersebut memang bekerja pada frekuensi range 2,4 GHz. Yang menjadi pertanyaan adalah mengapa harus pada frekuensi tersebut? Frekuensi range ini termasuk dalam kategori pita frekuensi ISM (*Industrial, Scientific, and Medical*). Pita frekuensi ISM ini memang dialokasikan oleh badan standardisasi dan regulasi untuk digunakan sebebas-bebasnya tanpa perlu diberi sistem perizinan (*unlicenses*). Maka dari itu, banyak sekali produk elektronik yang menggunakan pita frekuensi ini termasuk juga jaringan wireless.

Perangkat lain yang menggunakan frekuensi jenis ini juga cukup banyak, seperti microwave oven, cordless phone, wireless mic, dan banyak lagi perangkat lainnya. Biasanya perangkat yang menggunakan frekuensi ini adalah perangkat rumah tangga atau kedokteran yang hanya perlu memancarkan sinyal radio ber-*power* rendah. *Development* perangkat-perangkat yang menggunakan frekuensi jenis ini menjadi sangat pesat karena sifatnya yang bebas perizinan ini.

5. Mengapa 802.11a Menggunakan Frekuensi 5 GHz?

Pita frekuensi yang digunakan oleh standar ini tergolong dalam kategori UNII (*Unlicensed National Information Infrastructure*). Sama seperti pita frekuensi standar 802.11b/g, frekuensi ini juga tidak memerlukan perizinan untuk menggunakannya. Perbedaan yang paling mendasar dari kedua jenis frekuensi ini hanyalah sudah umum atau belumnya penggunaan frekuensi ini di masyarakat. Saat ini, frekuensi UNII 5 GHz ini masih jarang digunakan sehingga problem-problem seperti interferensi sangat jarang terjadi di sini.

6. Apakah WI-FI Itu?

WI-FI merupakan istilah yang diberikan untuk sistem wireless LAN yang menggunakan standar 802.11 yang ada saat ini. Istilah WI-FI diciptakan oleh sebuah organisasi bernama WI-FI alliance yang bekerja menguji dan memberikan sertifikasi untuk perangkat-perangkat WLAN.

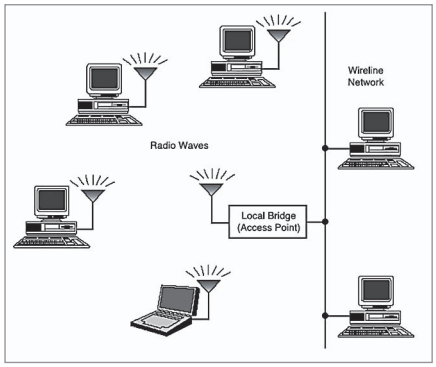
Perangkat wireless diuji berdasaarkan interoperabilitasnya dengan perangkat-perangkat wireless lain yang menggunakan standar yang sama. Setelah diuji dan lulus, sebuah perangkat akan diberi sertifikasi "WI-FI certified". Artinya perangkat ini bisa bekerja dengan baik dengan perangkat-perangkat wireless lain yang juga bersertifikasi ini.

Pada awalnya, sertifikasi WI-FI hanya diberikan pada perangkat wireless yang bekerja pada standar 802.11b. Namun, saat ini standar ini juga diberikan pada semua perangkat yang menggunakan standar 802.11. Sertifikasi WI-FI sudah dianggap sebagai sertifikasi standar untuk perangkat wireless yang ada saat ini. WI-FI sudah banyak digunakan di berbagai sektor seperti bisnis, akademis, perumahan, dan banyak lagi.

7. Apakah Access Point?

Access point atau yang lebih sering disebut dengan istilah AP merupakan sebuah perangkat penghubung antara jaringan *wire* dengan *wireless*. Maksudnya sebuah AP akan bertugas mengubah data yang lalu lalang di media kabel menjadi sinyal-sinyal radio yang dapat ditangkap oleh perangkat wireless. AP akan menjadi gerbang bagi jaringan wireless untuk dapat berkomunikasi dengan dunia luar maupun dengan antarsesama perangkat wireless di dalamnya.

Biasanya pada perangkat AP terdapat satu atau lebih *interface* untuk media kabel. Apakah port ethernet, port ADSL, Cable, line telepon biasa, dan banyak lagi. Interface media kabel tadi akan di-*bridging* oleh AP tersebut ke dalam



AP bertugas menghubungkan jaringan kabel dengan tanpa kabel.

bentuk sinyal-sinyal radio, sehingga perangkat wireless dengan kabel tadi dapat terkoneksi. AP biasanya memiliki sistem antena untuk mentransmisikan sinyal-sinyalnya. Sistem antenanya pun bermacam-macam.

Penggunaan AP yang banyak tentu akan meningkatkan kapasitas pengguna dan juga jarak coverage jaringan wireless Anda. Selain itu, Anda juga dapat menciptakan sebuah sistem *roaming* WLAN. Maksudnya para pengguna dapat bergerak ke sana-ke mari dengan bebas tanpa terputus koneksinya karena sinyal-sinyal komunikasinya dapat dilayani oleh beberapa AP yang berbeda. Sistem yang sama juga digunakan dalam jaringan telepon selular.

8. Apakah AP Selalu Diperlukan?

Access point sangat dibutuhkan jika Anda ingin membuat sebuah infrastruktur jaringan wireless. Dengan menggunakan AP, maka sebuah jaringan komunikasi akan terbentuk tidak hanya dua atau tiga perangkat saja yang dapat berkomunikasi tetapi cukup banyak yang dapat saling berbicara dengan perantara sinyal radio ini. Selain itu dengan menggunakan AP, jaringan kabel dengan wireless juga dapat berhubungan sehingga komunikasi jaringan menjadi lebih lebar.

Pengaplikasian AP yang banyak dilakukan saat ini adalah melakukan pembagian *bandwidth* Internet dari link Internet ADSL atau Kabel, sehingga dapat digunakan oleh banyak orang. AP juga dapat memperluas jangkauan jaringan Anda menjadi lebih lebar daripada jaringan kabel Anda yang ada.

Namun jika Anda ingin membangun koneksi hanya dengan sebuah perangkat

wireless lainnya, AP tidaklah mutlak diperlukan. Anda dapat mengoperasikan perangkat wireless Anda dalam mode *peer-to-peer* atau yang lebih dikenal dengan istilah mode *Ad-Hoc*. Tetapi, kekurangan dari komunikasi mode Ad-Hoc ini Anda tidak dapat membangun jaringan wireless yang luas karena memang sifatnya yang *Point-to-Point*.

Jarak jangkauannya pun tidak bisa terlalu jauh karena sistem WI-FI pada perangkat aplikasi tidaklah terlalu besar powernya. Selain itu, cukup sulit bagi Anda untuk mengatur *traffic* data Anda jika ingin berpindah-pindah lawan komunikasi. Jadi sebenarnya menggunakan AP untuk jaringan wireless sangat menguntungkan.

9. Berapa Banyak Pengguna yang Dapat Dilayani oleh Sebuah AP?

Anda akan sering menemukan dua batasan jika berhubungan dengan pertanyaan berapa banyak pengguna yang dapat dilayani oleh sebuah AP. Batasan pertama, yaitu limitasi dari perangkat AP itu sendiri. Sering kali produsen AP melakukan pembatasan jumlah pengguna yang dapat terkoneksi ke jaringan wireless yang dibentuknya. Biasanya tujuan dari limitasi ini adalah untuk menjaga kualitas jaringan wireless yang disediakannya. Namun Anda akan cukup kesulitan jika penggunanya sudah berjumlah banyak.

Batasan kedua adalah banyaknya data yang ingin lalu-lalang di dalam jaringan wireless tersebut. Sebuah AP juga memiliki batasan dalam menyediakan bandwidth untuk media wireless-nya. Ketika ada pengguna yang melakukan *download* atau *upload* data dalam jumlah besar, secara otomatis sesi yang dapat terbentuk untuk pengguna lain akan berkurang jumlahnya. Penyebabnya adalah bandwidth yang juga semakin kecil jatahnya untuk pengguna tersebut. Ketika bandwidth-nya tidak mencukupi untuk melayani pengguna lain, maka pengguna tersebut tidak akan dapat bergabung dengan jaringan wireless ini.

Problem terbatasnya jumlah pengguna yang dapat terkoneksi ke sebuah AP dapat diatasi dengan menambahkan perangkat AP lain dalam area jaringan wireless tersebut.

10. Berapa Banyak Pengguna yang Bisa Dilayani oleh Sistem WLAN?

Sistem WLAN, terlepas dari keterbatasan perangkat AP, dapat melayani pengguna dalam jumlah yang tidak terbatas. Para penggunanya dapat menambahkan AP-AP baru jika memang jumlah pengguna yang akan dilayaninya semakin membengkak. Dengan memasang banyak AP, maka banyak sekali keuntungan yang didapat. Anda bisa memanjakan pengguna jaringan wireless dengan bandwidth yang lega, pengguna juga dapat bebas berkeliaran di manapun mereka suka karena area *coverage*-nya sudah pasti lebih luas, dan jumlah pengguna yang dapat dilayani oleh jaringan ini juga lebih banyak.

Jadi sebenarnya sistem WLAN tidak pernah memberikan batasan berapa banyak yang dapat terkoneksi ke sebuah jaringan wireless. Semua tergantung pada kemampuan dan fasilitas perangkatnya.

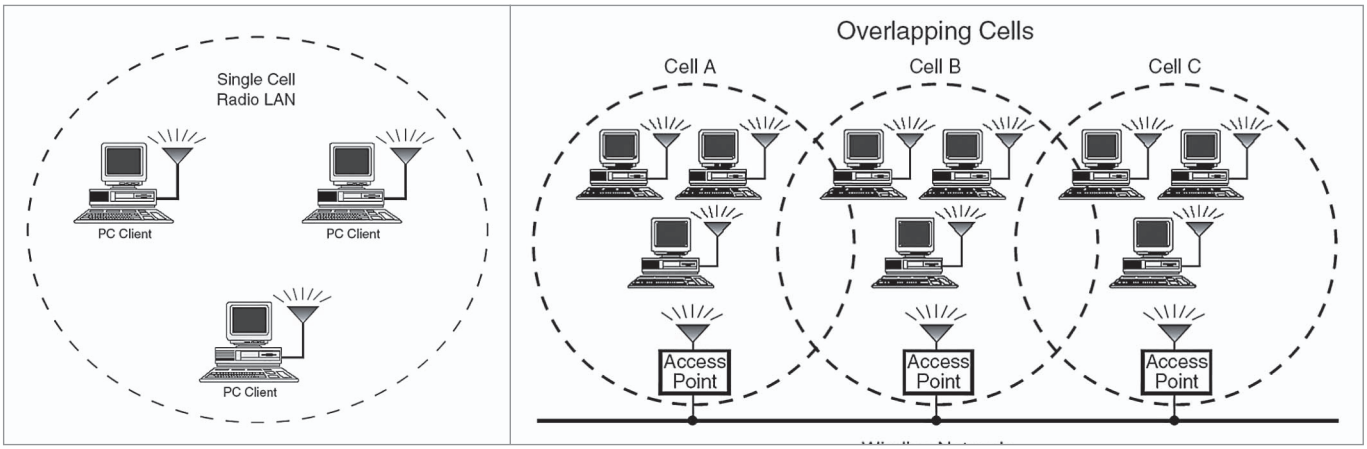
11. Apa Maksud dari Wireless Gateway?

Wireless gateway biasanya adalah julukan yang diberikan untuk sebuah perangkat wireless yang memiliki kemampuan bertindak sebagai gateway untuk menuju ke Internet atau ke jaringan lain. Wireless gateway biasanya berupa AP yang memiliki interkoneksi dengan media lain seperti ADSL, kabel, line telepon, dan banyak lagi. Di dalam perangkat wireless gateway biasanya pasti terdapat fasilitas pendukung seperti kemampuan NAT dan VPN. Fasilitas ini tidak akan Anda temukan pada perangkat wireless biasa selain wireless gateway.

12. Apakah Wireless SSID?

Anda mungkin sering mendengar istilah SSID pada segala sesuatu yang berhubungan dengan jaringan wireless. Sebenarnya apa *sih* SSID itu? SSID merupakan singkatan dari *Service Set Identifier*. Sebuah SSID memiliki fungsi untuk menamai sebuah jaringan wireless yang dipancarkan dari sebuah AP. Sistem penamaan ini adalah sistem kontrol pertama sebuah jaringan wireless. Maksudnya, dengan diberikannya sebuah nama, maka pengguna yang ingin bergabung dalam jaringan tersebut harus mengetahui nama ini terlebih dahulu.

Jika nama yang dimasukkan oleh klien pengguna sama dengan nama yang ada di AP maka jaringan wireless tersebut baru dapat diakses. Jika tidak, maka Anda tidak akan mendapatkan apa-apa



Dengan menggunakan perangkat AP lebih dari satu buah, membuat jaringan *wireless* Anda semakin skalabel dan pengguna akan lebih leluasa berkomunikasi data.

dalam jaringan tersebut meskipun sinyalnya bisa tertangkap.

Sistem penamaan SSID dapat diberikan maksimal sebesar 32 karakter. Karakter-karakter tersebut juga dibuat case sensitive sehingga SSID dapat lebih banyak variasinya.

13. Apa yang Dapat Anda Lakukan untuk Mengamankan WLAN?

Ada beberapa metode yang dapat Anda gunakan untuk "sedikit" mengamankan jaringan wireless Anda yang tak kasat mata ini. Dikatakan sedikit karena jaringan wireless memang sangat rentan dari segi keamanannya. Karena media ini bekerja pada udara terbuka dan bebas, maka sinyal-sinyal komunikasi Anda ini dapat dengan mudah ditangkap oleh siapapun.

Untuk itu, ada beberapa teknik yang dapat Anda gunakan untuk lebih mempersulit para pengganggu untuk mengacau jaringan wireless Anda. Metode tersebut adalah WEP, WPA, dan 802.1x.

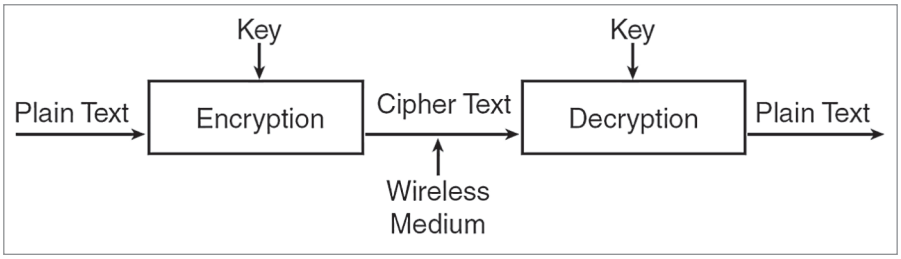
14. Apa Itu WEP?

Teknik pengaman jaringan wireless yang satu ini merupakan kepanjangan dari *Wired Equivalent Privacy*. Teknik ini merupakan fasilitas opsional yang ada di dalam standar 802.11. Fitur ini akan membuat jaringan wireless Anda mempunyai keamanan yang hampir sama dengan apa yang ada dalam jaringan kabel. WEP menggunakan sistem enkripsi untuk memproteksi pengguna WLAN dalam level yang paling dasar. WEP memungkinkan administrator jaringan wireless membuat *encription key* yang akan digunakan untuk mengenkripsi data sebelum dikirimkan melalui jalan udara. Encription key ini biasanya dibuat dari 64 bit key awal dan dipadukan dengan algoritma enkripsi RC4.

Ketika fasilitas WEP diaktifkan, maka semua perangkat wireless (AP dan client) yang ada di jaringan harus dikonfigurasi dengan menggunakan key yang sama. Hak akses dari seseorang atau sebuah perangkat akan ditolak jika key yang dimasukkan tidak sama.

15. Apa Itu WPA?

WI-FI Protected Access atau disingkat dengan istilah WPA, merupakan teknik pengaman jaringan wireless LAN yang diklaim lebih canggih dari WEP. Dengan disertai teknik enkripsi yang lebih *advanced* dan tambahan pengaman berupa otentikasi dari penggunanya, maka WPA akan jauh lebih hebat mengamankan Anda pengguna WLAN.



Sistem enkripsi pada *wireless* membuat media ini sedikit lebih aman karena tidak akan mudah untuk dibaca meskipun sudah berhasil didapat.

16. Apa Itu 802.1x?

Teknik pengaman yang satu ini akan mengharuskan semua pengguna jaringan wireless untuk melakukan proses otentikasi terlebih dahulu sebelum dapat bergabung dalam jaringan. Sistem otentikasinya dapat dilakukan dengan banyak cara, namun sistem otentikasi menggunakan pertukaran key secara dinamik. Sistem pertukaran key secara dinamik ini dapat dibuat dengan menggunakan *Extensible Authentication Protocol* (EAP). Sistem EAP ini sudah cukup banyak terdapat di dalam implementasi fasilitas-fasilitas di RADIUS.

Dalam metode ini, *software key management* dimasukkan pada perangkat WLAN client. Dalam asosiasi pertama dengan perangkat AP, software tersebut akan memberitahukan pengguna untuk memasukkan identitas jaringan WLAN yang ingin dimasukki seperti *username password* misalnya. Identitas ini kemudian diteruskan ke EAP atau RADIUS server melalui AP untuk proses otentikasi. Ketika authentikasi berhasil, seperangkat encription key diberikan untuk perangkat AP dan juga client untuk dapat saling berkomunikasi. Namun, key ini hanya berlaku dalam satu sesi komunikasi saja. Ketika penggunanya melakukan roaming atau berpindah-pindah AP, maka encription key yang dinamik ini akan dikirimkan oleh AP yang memilikinya ke seluruh AP yang terkoneksi dengannya.

Wireless atau Kabel

Jaringan wireless LAN memang cukup menyimpan banyak pertanyaan bagi pengguna yang masih tergolong baru. Adalah sangat penting untuk mengetahui benar-benar apa dan bagaimana sebenarnya teknologi ini bekerja melayani Anda. Teorinya dalam penerapan memang lebih banyak daripada hanya menarikkan seutas kabel antardua perangkat jaringan. Apalagi kalau sudah bermain-main dengan frekuensi dan interferensi, tentu akan lebih memusingkan daripada media kabel.

Namun tidak ada salahnya untuk Anda kenali lebih dalam karena jika sudah mengetahuinya, banyak manfaat yang Anda dapatkan. Banyak solusi yang sebelumnya tidak terpikirkan oleh Anda malah merupakan solusi yang brilian bagi perusahaan maupun pribadi Anda.

Selain solusi brilian, teknologi WLAN juga sering kali menawarkan nilai ekonomis yang tinggi untuk penggunanya. Anda tidak perlu membayar orang untuk menarik kabel, tidak perlu membeli berol-rol kabel, tidak perlu membeli konektor, dan masih banyak lagi kenyamanan yang ditawarkan WLAN. Banyak yang akan Anda dapatkan jika mengetahui serba-serbi media wireless lebih banyak. Selamat belajar! ■

LEBIH LANJUT

www.smarthomeforum.com
➔Situs mengenai teknologi-teknologi seputar komunikasi data.
www.computerworld.com
➔Situs mengenai FAQ seputar *wireless* LAN dan problemnya.
www.intel.com
➔ Anda bisa menemukan banyak *whitepaper* mengenai *wireless* LAN di sini.

Kita telah melihat bahwa *proxy* memberikan dampak positif terhadap keamanan dan kinerja. Namun, proxy juga mempunyai dampak negatif berikut...

Gunung Sarjono

Bagian 2 dari 2 Artikel

Proxy: Apa dan Bagaimana?

Seperti mata uang yang mempunyai dua sisi, proxy menyebabkan beberapa masalah sekuriti berikut: proxy dapat membuat *single point of failure*; software client sering kali harus dapat bekerja dengan proxy (hanya sistem firewall dan proxy tingkat lanjut yang dapat bekerja transparan pada jaringan); proxy harus ada untuk semua layanan; proxy tidak melindungi inti sistem operasi; konfigurasi *default* sering kali dioptimalkan untuk kinerja bukannya sekuriti.

Single Point of Failure

Bersamaan dengan kontrol terpusat, maka ada kesalahan terpusat (*single point of failure*). Jika *hacker* dapat mematikan proxy Anda, seluruh organisasi dapat terputus dari Internet. Proxy, router, dan *firewall* semua mengalami hal ini. Pada router masalah mudah diatasi dengan menggunakan lebih dari satu rute ke Internet. Firewall jauh lebih aman dibanding proxy karena mereka menyediakan filtering paket untuk menghilangkan masalah yang disebabkan oleh *denial-of-service*. Namun, proxy murni tidak menyertakan fungsi untuk melindungi diri mereka dari serangan sehingga mereka sangat rentan baik terhadap penyusupan dan denial-of-service.

Proxy server modern biasanya menyertakan fitur *hot-failover,* di mana proxy kedua dengan koneksi jaringan yang sama secara kontinyu meng-*query* proxy yang "hidup" dan mengambil alamat IP-nya jika mati. Yang lain menggunakan fitur *load-balancing* untuk menyediakan beberapa proxy yang semua digunakan pada saat bersamaan. Fitur Load Balancing pada *operating system* dapat dikonfigurasi bersama *software* proxy server untuk membuat proxy *fault-tolerant* semacam ini.

Client Harus Menggunakan Proxy

Client yang menggunakan proxy harus ada untuk setiap layanan yang ingin Anda proxy. Sebagai contoh, *web browser* Anda harus mendukung koneksi ke proxy server dengan mengonfigurasi ke proxy mana semua *reguest* harus dikirimkan. Jika software client tidak dapat dikonfigurasi untuk menggunakan proxy, layanan proxy tidak dapat digunakan kecuali dengan *Network Address Translator*. Ini bisa menjadi masalah besar untuk layanan seperti FTP di mana software client yang disertakan bersama kebanyakan *operating system* tidak mendukung koneksi ke proxy server. Namun, Anda bisa membeli proxy client.

Layanan proxy yang mempunyai *address translating firewall* dapat mengatasi mengatasi ini karena mereka dapat memodifikasi alamat jaringan *inbound* dan *outbound*. Ini berarti client tidak perlu tahu atau dikonfigurasi untuk menggunakan proxy yang ada sebagai bagian dari address translating firewall.

Proxy Harus Ada untuk Setiap Layanan

Layanan proxy yang berbeda dibutuhkan untuk setiap protokol layanan. *Network Address Translation* bersifat universal dan dapat bekerja dengan semua protokol kecuali dengan mereka yang mengandalkan alamat IP atau membutuhkan kemampuan untuk membuka *back channel* untuk client. Protokol di mana layanan proxy tidak tersedia tidak dapat dihubungkan melalui proxy, kecuali dengan layanan proxy TCP generik (seperti proxy SOCKS generik) yang

bekerja mirip dengan Network Address Translator. Namun, layanan seperti ini tidak dapat memfilter content.

Adanya banyak layanan membuat tidak ada pemilteran content yang efektif. Layananan *streaming* seperti RealAudio atau RealVideo sangat sulit untuk difilter karena isinya kerena isinya harus dialiri secara *real time*, dan interupsi pada aliran data akan membuat sisa aliran tidak dapat dibaca. Karena content seperti ini tidak dapat difilter, maka harus diblokir jika dianggap membahayakan keamanan.

Proxy Tidak Melindungi Inti Operating System

Proxy server berdasarkan pada web server dan seperti web server, mereka beroperasi pada *Application Layer*—di atas *Network* dan *Transport Layer*. Ini berarti mereka tidak melakukan apa-apa selain memfilter paket TCP/IP yang tiba di server, dan mereka tidak mencampuri layanan *Application Layer* yang lain seperti *file sharing* atau *remote procedure call*.

Hal ini membuat komputer terbuka terhadap *hacking*, kecuali jika Anda mengambil langkah lain untuk mengamankan komputer. Walaupun kebanyakan *operating system* modern mendukung pemilteran paket, tetapi filter mereka tidak sekuat *firewall* sungguhan. Yang perlu Anda pastikan adalah hanya port publik untuk layanan yang Anda proxy yang dibuka.

Beberapa pakar keamanan menganjurkan, supaya menjalankan layanan sedikit mungkin pada firewall dan memisahkan fungsi proxy pada mesin terpisah dengan asumsi bahwa filter harus sesederhana mungkin supaya tidak dieksploitasi.

PROXY BEST PRACTICE

■ *Proxy* berguna untuk sejumlah tujuan yang berbeda, dan untuk alasan keamanan sering kali kinerja atau penyebaran koneksi menempati kursi belakang. Proxy dapat sangat berbahaya jika mereka digunakan dengan tidak benar (*oke*, memang orang tidak benar-benar luka hanya bahaya dalam konteks legalitas) karena *hacker* dapat mengeksploitasi mereka supaya aktivitasnya tampak seolah-olah datang dari dalam jaringan Anda. Ini dapat membuat perusahaan Anda bertanggung jawab atas aktivitas mereka.

Gunakan Firewalll Sungguhan

Hal paling penting yang dapat dilakukan untuk melindungi diri Anda sendiri adalah dengan menggunakan fungsi proxy pada *firewall* sungguhan atau menaruh firewall di depan proxy server Anda untuk melindunginya. Tidak ada alasan mengapa proxy server harus terhubung langsung ke jaringan eksternal kecuali jika proxy digunakan untuk *reverse proxy load balancing* suatu situs web.

Matikan Routing

Jika Anda menggunakan proxy sebagai pelindung utama terhadap *hacker*, pastikan untuk mematikan routing melalui proxy. Jika Anda menyalakan routing melalui proxy, proxy tidak akan melakukan fungsi sekuriti secara signifikan karena client Anda semua akan dapat dilihat dari Internet. Fitur penyembunyian client pada proxy menggandalkan penonaktifan routing untuk mencegah sejumlah serangan protokol *low-level*.

Biasanya routing pada proxy dimatikan, tetapi kadang-kadang Anda membutukan suatu layanan atau protokol yang tidak mempunyai layanan proxy khusus atau tidak dapat di-proxy. Jangan tergoda dengan begitu saja menyalakan routing. Jika layanan yang Anda butuhkan tidak dapat diproxy, gunakan Network Address Translation. Jika layanan tersebut tidak dapat ditranslasi maupun di-proxy, jangan gunakan sama sekali.

Amankan Dasar Operating System

Mengamankan dasar *operating system* sangat penting dalam menggunakan proxy secara efektif sebagai perangkat pengaman. Jika hacker tidak dapat mengeksploitasi server di mana proxy berjalan, mereka tidak dapat mengganti setting sekuriti proxy untuk melewatinya.

Ini merupakan hal yang penting terutama dalam lingkungan Unix dan Windows. Kedua operating system ini terkenal rentan terhadap *hacking*, sehingga proxy yang berjalan pada mereka juga sama rentannya.

Gunakan izin sekuriti yang kuat dan juga pemilteran port dan protokol pada operating system untuk memastikan proxy server hanya melayani protokol yang diinginkan. Cari tahu informasi hacking terakhir untuk operating system Anda dan pastikan untuk menggunakan patch dan *hot fix* pada server sekuriti eksternal begitu mereka dikeluarkan. Lebih penting bagi server publik untuk aman daripada stabil. *Crash* yang terjadi pada waktu menggunakan *path* atau *hotfix* yang belum diuji hanya menyebabkan hilangnya layanan secara sementara—tidak menyebabkan bobolnya keamanan.

Matikan Akses Eksternal

Jangan pernah izinkan client jaringan eksternal untuk ter-proxy melalui server Anda, walaupun jika hal ini terlihat masuk akal bagi *remote user*. Dengan memberikan akses eksternal ke proxy server, itu memungkinkan hacker untuk mengeksploitasi proxy server Anda untuk menutupi koneksi IP mereka dan membuatnya tampak seolah-olah proxy server Anda yang melakukan serangan. Ini dapat membuat Anda bertanggung jawab atas kerusakan yang mereka lakukan.

Matikan Akses yang tidak dibutuhkan

Jangan jalankan semua layanan publik pada mesin yang sama dengan proxy server. Aturan umum ini penting, terutama pada waktu menggunakan mekanisme sekuriti seperti proxy server. Jika layanan seperti FTP atau SMTP memungkinkan hacker untuk mengakses proxy server, hacker tersebut dapat mematikan *setting* sekuriti proxy server untuk mendapatkan akses lebih lanjut ke jaringan Anda. Namun jika layanan ini terbagi ke beberapa mesin, serangan khusus FTP hanya akan memberikan akses ke FTP server, bukan seluruh jaringan.

Masalahnya adalah bahwa eksploitasi dapat muncul pada berbagai level, dan jika Anda membuat proxy server di belakang filter, *hacker* akan ada di belakang filter jika ia mengeksploitasi proxy. Dengan menggunakan firewall yang terintegrasi dengan proxy server, filter masih dapat melindungi jaringan bahkan jika layanan proxy dieksploitasi.

Longgarnya Konfigurasi Default

Banyak paket *software proxy server* yang mempunyai konfigurasi *default* longgar yang dapat menyebabkan masalah keamanan serius. Sebagai contoh, WinGate, proxy server yang paling populer untuk lingkungan rumah dan kantor kecil, lebih sering digunakan untuk membagi satu koneksi Internet bukannya untuk keamanan. Oleh karena itu, pembuat software membuatnya mudah untuk di-*setup* oleh orang yang tidak mengerti proxy, dan diset secara default untuk bekerja dengan semua protokol umum.

Untuk versi sebelum 3.0, instalasi default membuka proxy Winsock ke *interface* eksternal, yang memungkinkan hacker untuk terhubung ke interface eksternal tersebut seolah-olah mereka adalah client internal. Hacker kemudian dapat menggunakan proxy untuk terhubung ke layanan web atau Internet yang lain seolah-olah mereka bekerja langsung dari komputer user (yang tidak dicurigai). Ini otomatis menutupi koneksi mereka. Konfigurasi default versi 3.0 mematikan koneksi yang datang dari interface eksternal.

Banyak proxy server mempunyai masalah konfigurasi default yang longgar karena mereka seringkali didesain untuk pengguna komputer yang kurang pengalaman dan menaruh kinerja dan fungsionalitas di depan keamanan. Kebanyakan dapat dikonfigurasi dengan benar, tetapi *user* sering mengabaikan software tersebut setelah selesai diinstalasi.

Masalah Proxy Terhadap Kinerja

Proxy server mempunyai satu kekurangan pada kinerja, yaitu proxy server membuat *bottleneck*. Seperti firewall atau router, satu koneksi proxy server ke Internet dapat membuat bottleneck jika tidak di-*upgrade* ketika jumlah user jaringan bertambah. Walaupun proxy awalnya meningkatkan kinerja melalui mekanisme *caching*, Anda akan membuat semua orang menunggu di belakang mesin yang lambat jika Anda mendapatkan lebih banyak klien dari yang dapat didukung oleh server.

Namun, hati-hati dalam menyalahkan proxy Anda jika terjadi bottleneck yang sebenarnya disebabkan oleh jalur Internet yang lambat. Jika Anda hanya mempunyai satu koneksi Internet, dan itu adalah T1 (1,5 MB) atau yang lebih lambat, semua komputer yang betul-betul memenuhi kebutuhan minimum operating system dan proxy server sudah cukup cepat dalam menangani beban yang ada. Bottleneck proxy hanya dapat terjadi bila koneksi jaringan lebih cepat dari 1,5 MB/s atau pada waktu ada yang salah dengan proxy server.

Masalah ini mudah diatasi dengan menambah lebih banyak proxy server. Tidak seperti situs web atau server publik, proxy server todal perlu mempunyai konfigurasi yang persis sama dengan mesin yang lain. Anda dapat menghubungkan secara langsung berapa pun proxy server yang Anda inginkan ke koneksi jaringan eksternal dan memberikan masing-masing klien di dalam jaringan Anda ke salah salah proxy server.

Sebagai contoh, jika Anda mempunyai empat proxy server, hubungkan tiap klien keempat ke proxy server yang sama. Anda akan kehilangan beberapa manfaat caching karena client pada proxy berbeda yang mengakses suatu situs tidak akan membuat situs itu tersedia untuk proxy yang lain.

Anda dapat menggunakan software yang canggih dan TCP/IP load balancing untuk menangani koneksi ke beberapa proxy, tetapi itu membutuhkan biaya yang patut dipertimbangkan dan tidaklah jauh efisien. Namun, ini menyediakan redundansi proxy, karena jika tidak user dapat kehilangan layanan jika proxy mereka mati.

Explicit vs Transparent Proxy

Kebanyakan proxy, terutama proxy HTTP, butuh supaya software client dikonfigurasi secara eksplisit untuk menggunakan proxy server dalam mengakses data (seperti halaman web) dari jaringan luar. Ini berarti bukan hanya setiap web browser, FTP client, atau aplikasi videophone yang harus bisa menggunakan proxy server (banyak yang tidak, karena telah diprogram dengan asumsi ada akses bebas ke Internet), tetapi juga system administrator harus mengonfigurasi semua aplikasi pada komputer client dalam jaringan supaya menggunakan proxy atau mengajari user bagaimana melakukannya.

Masalah konfigurasi tidak menjadi beban bagi network administrator karena web browser modern mempunyai kemampuan untuk mendeteksi setting proxy pada jaringan secara otomatis. Namun software client lain, seperti FTP atau Net2phone, tidak diprogram untuk melakukan itu. Walaupun fitur tersebut menguntungkan network administrator, ada cara lebih baik bagi protokol lain juga dan tidak perlu mengonfigurasi atau mengubah software client jaringan—*transparent proxy*.

Transparent Proxy Mengganti Aturan

Semua *firewall* modern dapat mengalihkan *request* yang datang ke port atau komputer tertentu atau komputer interior tertentu yang akan memenuhi request tersebut (seperti web server pada jaringan interior yang diproteksi oleh firewall). Dengan cara yang sama, firewall dapat menginterupsi dan mengalihkan *traffic outgoing* ke komputer tertentu, seperti *proxy server* untuk request web. Komputer client tidak perlu tahu bahwa traffic diinterupsi karena firewall dapat mengalihkan respon proxy server ke client yang meminta seolah-olah tidak ada apapun yang terjadi (menggunakan mekanisme *Network Address Translation* yang sekarang tersebar luas). Anda dapat menemukan di Internet instruksi untuk menggunakan fitur firewall oada BSD atau Linux bersama dengan paket proxy seperti Jigsaw. ■

LEBIH LANJUT

http://www.atomintersoft.com/products/alive-proxy/proxy-list/transparent/
➔Daftar *transparent proxy server* publik yang *free*.

Routing protokol jenis yang satu ini sangat penting untuk Anda pelajari, karena penggunaannya sangat umum dan sudah tersebar di mana-mana. Kenalilah lebih dalam lagi.

Hayri

Bagian 1 dari 2 Artikel

OSPF, Routing Protokol untuk Jaringan Lokal

Setelah membahas sekian banyak jenis routing protokol yang umum digunakan dalam jaringan, kali ini yang akan dibahas adalah sebuah routing protokol yang paling terkenal dalam dunia jaringan lokal berskala menengah hingga besar. Khususnya para administrator jaringan berskala menengah sampai besar, paling tidak pernah mengenal routing protokol yang satu ini walaupun belum pernah mengimplementasikannya. Routing protokol ini bernama *Open Shortest Path First* atau yang lebih sering disebut dengan nama OSPF.

Mengapa dikatakan paling terkenal? Yang menyebabkan OSPF menjadi terkenal adalah karena routing protokol ini notabene adalah yang paling cocok digunakan dalam jaringan lokal berskala sedang hingga *enterprise*. Misalnya di kantor-kantor yang menggunakan lebih dari 50 komputer beserta perangkat-perangkat lainnya, atau di perusahaan dengan banyak cabang dengan banyak klien komputer, perusahaan multinasional dengan banyak cabang di luar negeri, dan banyak lagi. Mengapa dikatakan paling cocok? Karena OSPF memiliki tingkat skalabilitas, reliabilitas, dan kompatibilitas yang tinggi. Mengapa demikian? Nanti akan dibahas satu per satu di bawah.

Selain paling cocok, kemampuan routing protokol ini juga cukup hebat dengan disertai banyak fitur pengaturan. Sebuah routing protokol dapat dikatakan memiliki kemampuan hebat selain dapat mendistribusikan informasi routing dengan baik juga harus dapat dengan mudah diatur sesuai kebutuhan penggunanya. OSPF memiliki semua ini dengan berbagai pernak-pernik pengaturan dan fasilitas di dalamnya.

OSPF memang sangat banyak penggunanya karena fitur dan kemampuan yang cukup hebat khususnya untuk jaringan internal sebuah organisasi atau perusahaan. Dibandingkan dengan RIP dan IGRP, yang sama-sama merupakan routing protokol jenis IGP (*Interior Gateway Protocol*), OSPF lebih *powerful*, skalabel, fleksibel, dan lebih kaya akan fitur.

Apa Sebenarnya OSPF?

OSPF merupakan sebuah routing protokol berjenis IGP yang hanya dapat bekerja dalam jaringan internal suatu ogranisasi atau perusahaan. Jaringan internal maksudnya adalah jaringan di mana Anda masih memiliki hak untuk menggunakan, mengatur, dan memodifikasinya. Atau dengan kata lain, Anda masih memiliki hak administrasi terhadap jaringan tersebut. Jika Anda sudah tidak memiliki hak untuk menggunakan dan mengaturnya, maka jaringan tersebut dapat dikategorikan sebagai jaringan eksternal.

Selain itu, OSPF juga merupakan routing protokol yang berstandar terbuka. Maksudnya adalah routing protokol ini bukan ciptaan dari vendor manapun. Dengan demikian, siapapun dapat menggunakannya, perangkat manapun dapat kompatibel dengannya, dan di

manapun routing protokol ini dapat diimplementasikan.

OSPF merupakan routing protokol yang menggunakan konsep hirarki routing, artinya OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan area. Dengan menggunakan konsep hirarki routing ini sistem penyebaran informasinya menjadi lebih teratur dan tersegmentasi, tidak menyebar ke sana ke mari dengan sembarangan.

Efek dari keteraturan distribusi routing ini adalah jaringan yang penggunaan *bandwidth*-nya lebih efisien, lebih cepat mencapai konvergensi, dan lebih presisi dalam menentukan rute-rute terbaik menuju ke sebuah lokasi. OSPF merupakan salah satu routing protocol yang selalu berusaha untuk bekerja demikian.

Teknologi yang digunakan oleh routing protokol ini adalah teknologi *link-state* yang memang didesain untuk bekerja dengan sangat efisien dalam proses pengiriman update informasi rute. Hal ini membuat routing protokol OSPF menjadi sangat cocok untuk terus dikembangkan menjadi *network* berskala besar. Pengguna OSPF biasanya adalah para administrator jaringan berskala sedang sampai besar. Jaringan dengan jumlah router lebih dari sepuluh buah, dengan banyak lokasi-lokasi remote yang perlu juga dijangkau dari pusat, dengan jumlah pengguna jaringan lebih dari lima ratus perangkat komputer, mungkin sudah layak menggunakan routing protocol ini.

Bagaimana OSPF Membentuk Hubungan dengan Router Lain?

Untuk memulai semua aktivitas OSPF dalam menjalankan pertukaran informasi routing, hal pertama yang harus dilakukannya adalah membentuk sebuah komunikasi dengan para router lain. Router lain yang berhubungan langsung atau yang berada di dalam satu jaringan dengan router OSPF tersebut disebut dengan *neighbour router* atau router tetangga.

Langkah pertama yang harus dilakukan sebuah router OSPF adalah harus membentuk hubungan dengan neighbour router. Router OSPF mempunyai sebuah mekanisme untuk dapat menemukan router tetangganya dan dapat membuka hubungan. Mekanisme tersebut disebut dengan istilah *Hello protocol*.

Dalam membentuk hubungan dengan tetangganya, router OSPF akan mengirimkan sebuah paket berukuran kecil secara periodik ke dalam jaringan atau ke sebuah perangkat yang terhubung langsung dengannya. Paket kecil tersebut dinamai dengan istilah *Hello packet*. Pada kondisi standar, Hello packet dikirimkan berkala setiap 10 detik sekali (dalam *media broadcast multiaccess*) dan 30 detik sekali dalam media *Point-to-Point*.

Hello packet berisikan informasi seputar pernak-pernik yang ada pada router pengirim. Hello packet pada umumnya dikirim dengan menggunakan multicast address untuk menuju ke semua router yang menjalankan OSPF (IP multicast 224.0.0.5). Semua router yang menjalankan OSPF pasti akan mendengarkan protokol hello ini dan juga akan mengirimkan hello packet-nya secara berkala. Cara kerja dari Hello protocol dan pembentukan neighbour router terdiri dari beberapa jenis, tergantung dari jenis media di mana router OSPF berjalan.

OSPF Bekerja pada Media Apa Saja?

Seperti telah dijelaskan di atas, OSPF harus membentuk hubungan dulu dengan router tetangganya untuk dapat saling berkomunikasi seputar informasi routing. Untuk membentuk sebuah hubungan dengan router tetangganya, OSPF mengandalkan Hello protocol. Namun uniknya cara kerja Hello protocol pada OSPF berbeda-beda pada setiap jenis media. Ada beberapa jenis media yang dapat meneruskan informasi OSPF, masing-masing memiliki karakteristik sendiri, sehingga OSPF pun bekerja mengikuti karakteristik mereka. Media tersebut adalah sebagai berikut:

- **Broadcast Multiaccess**

Media jenis ini adalah media yang banyak terdapat dalam jaringan lokal atau LAN seperti misalnya ethernet, FDDI, dan *token ring*. Dalam kondisi media seperti ini, OSPF akan mengirimkan *traffic multicast* dalam pencarian router-router neighbour-nya. Namun ada yang unik dalam proses pada media ini, yaitu akan terpilih dua buah router yang berfungsi sebagai *Designated Router* (DR) dan *Backup Designated Router* (BDR). Apa itu DR dan BDR akan dibahas berikutnya.

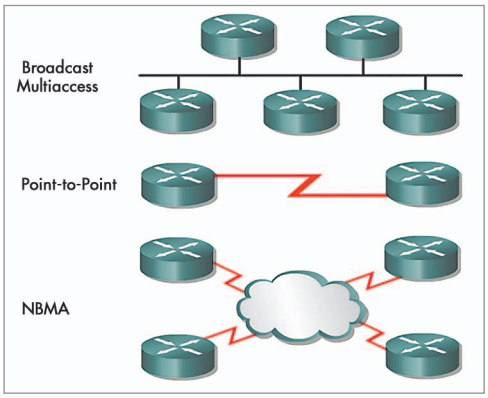
- **Point-to-Point**

Teknologi *Point-to-Point* digunakan pada kondisi di mana hanya ada satu router lain yang terkoneksi langsung dengan sebuah perangkat router. Contoh dari teknologi ini misalnya link serial. Dalam kondisi Point-to-Point ini, router OSPF tidak perlu membuat Designated Router dan Back-up-nya karena hanya ada satu router yang perlu dijadikan sebagai neighbour. Dalam proses pencarian neighbour ini, router OSPF juga akan melakukan pengiriman Hello packet dan pesan-pesan lainnya menggunakan alamat multicast bernama AllSPFRouters 224.0.0.5.

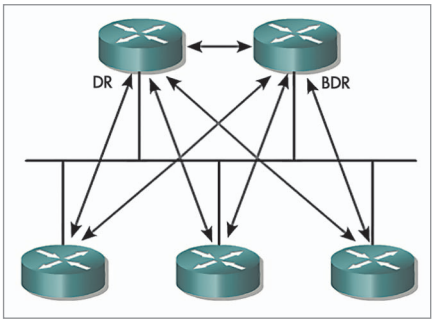
- **Point-to-Multipoint**

Media jenis ini adalah media yang memiliki satu interface yang menghubungkannya dengan banyak tujuan. Jaringan-jaringan yang ada di bawahnya dianggap sebagai serangkaian jaringan Point-to-Point yang saling terkoneksi langsung ke perangkat utamanya. Pesan-pesan routing protocol OSPF akan direplikasikan ke seluruh jaringan Point-to-Point tersebut.

Pada jaringan jenis ini, traffic OSPF juga dikirimkan menggunakan alamat IP multicast. Tetapi yang membedakannya dengan media berjenis broadcast multiaccess adalah tidak adanya pemilihan Designated dan Backup Designated Router karena sifatnya yang tidak meneruskan broadcast.



Berbagai media dapat dilayani oleh OSPF, namun cara kerja pada masing-masing media juga berbeda.



Sebagai juru bicara dalam jaringan *broadcast multiaccess*, DR dan BDR harus menjawab semua kebutuhan informasi OSPF dari router-router yang ada di dalam sebuah jaringan.

- **Nonbroadcast Multiaccess (NBMA)**

Media berjenis *Nonbroadcast multiaccess* ini secara fisik merupakan sebuah serial line biasa yang sering ditemui pada media jenis Point-to-Point. Namun secara faktanya, media ini dapat menyediakan koneksi ke banyak tujuan, tidak hanya ke satu titik saja. Contoh dari media ini adalah X.25 dan *frame relay* yang sudah sangat terkenal dalam menyediakan solusi bagi kantor-kantor yang terpencar lokasinya. Di dalam penggunaan media ini pun dikenal dua jenis penggunaan, yaitu jaringan *partial mesh* dan *fully mesh*.

OSPF melihat media jenis ini sebagai media broadcast multiaccess. Namun pada kenyataannya, media ini tidak bisa meneruskan broadcast ke titik-titik yang ada di dalamnya. Maka dari itu untuk penerapan OSPF dalam media ini, dibutuhkan konfigurasi DR dan BDR yang dilakukan secara manual. Setelah DR dan BDR terpilih, router DR akan mengenerate LSA untuk seluruh jaringan.

Dalam media jenis ini yang menjadi DR dan BDR adalah router yang memiliki koneksi langsung ke seluruh router tetangganya. Semua traffic yang dikirimkan dari router-router neighbour akan direplikasikan oleh DR dan BDR untuk masing-masing router dan dikirim dengan menggunakan alamat unicast atau seperti layaknya proses OSPF pada media Point-to-Point.

Bagaimana Proses OSPF Terjadi?

Secara garis besar, proses yang dilakukan routing protokol OSPF mulai dari awal hingga dapat saling bertukar informasi ada lima langkah. Berikut ini adalah langkah-langkahnya:

1. Membentuk Adjacency Router

Adjacency router arti harafiahnya adalah router yang bersebelahan atau yang terdekat. Jadi proses pertama dari router OSPF ini adalah menghubungkan diri dan saling berkomunikasi dengan para router terdekat atau neighbour router. Untuk dapat membuka komunikasi, Hello protocol akan bekerja dengan mengirimkan Hello packet.

Misalkan ada dua buah router, Router A dan B yang saling berkomunikasi OSPF. Ketika OSPF kali pertama bekerja, maka kedua router tersebut akan saling mengirimkan Hello packet dengan alamat multicast sebagai tujuannya. Di dalam Hello packet terdapat sebuah field yang berisi Neighbour ID. Misalkan router B menerima Hello packet lebih dahulu dari router A. Maka Router B akan mengirimkan kembali Hello packet-nya dengan disertai ID dari Router A.

Ketika router A menerima hello packet yang berisikan ID dari dirinya sendiri, maka Router A akan menganggap Router B adalah adjacent router dan mengirimkan kembali hello packet yang telah berisi ID Router B ke Router B. Dengan demikian Router B juga akan segera menganggap Router A sebagai adjacent routernya. Sampai di sini adjacency router telah terbentuk dan siap melakukan pertukaran informasi routing.

Contoh pembentukan adjacency di atas hanya terjadi pada proses OSPF yang berlangsung pada media Point-to-Point. Namun, prosesnya akan lain lagi jika OSPF berlangsung pada media broadcast multiaccess seperti pada jaringan ethernet. Karena media broadcast akan meneruskan paket-paket hello ke seluruh router yang ada dalam jaringan, maka adjacency router-nya tidak hanya satu. Proses pembentukan adjacency akan terus berulang sampai semua router yang ada di dalam jaringan tersebut menjadi adjacent router.

Namun apa yang akan terjadi jika semua router menjadi adjacent router? Tentu komunikasi OSPF akan meramaikan jaringan. *Bandwidth* jaringan Anda menjadi tidak efisien terpakai karena jatah untuk data yang sesungguhnya ingin lewat di dalamnya akan berkurang. Untuk itu pada jaringan broadcast multiaccess akan terjadi lagi sebuah proses pemilihan router yang menjabat sebagai "juru bicara" bagi router-router lainnya. Router juru bicara ini sering disebut dengan istilah *Designated Router*. Selain router juru bicara, disediakan juga back-up untuk router juru bicara ini. Router ini disebut dengan istilah Backup Designated Router. Langkah berikutnya adalah proses pemilihan DR dan BDR, jika memang diperlukan.

2. Memilih DR dan BDR (jika diperlukan)

Dalam jaringan broadcast multiaccess, DR dan BDR sangatlah diperlukan. DR dan BDR akan menjadi pusat komunikasi seputar informasi OSPF dalam jaringan tersebut. Semua paket pesan yang ada dalam proses OSPF akan disebarkan oleh DR dan BDR. Maka itu, pemilihan DR dan BDR menjadi proses yang sangat kritikal. Sesuai dengan namanya, BDR merupakan "shadow" dari DR. Artinya BDR tidak akan digunakan sampai masalah terjadi pada router DR. Ketika router DR bermasalah, maka posisi juru bicara akan langsung diambil oleh router BDR. Sehingga perpindahan posisi juru bicara akan berlangsung dengan smooth.

Proses pemilihan DR/BDR tidak lepas dari peran penting Hello packet. Di dalam Hello packet ada sebuah *field* berisikan ID dan nilai Priority dari sebuah router. Semua router yang ada dalam jaringan broadcast multiaccess akan menerima semua Hello dari semua router yang ada dalam jaringan tersebut pada saat kali pertama OSPF berjalan. Router dengan nilai Priority tertinggi akan menang dalam pemilihan dan langsung menjadi DR. Router dengan nilai Priority di urutan kedua akan dipilih menjadi BDR. Status DR dan BDR ini tidak akan berubah sampai salah satunya tidak dapat berfungsi baik, meskipun ada router lain yang baru bergabung dalam jaringan dengan nilai Priority-nya lebih tinggi.

Secara *default*, semua router OSPF akan memiliki nilai Priority 1. Range Priority ini adalah mulai dari 0 hingga 255. Nilai 0 akan menjamin router tersebut tidak akan menjadi DR atau BDR, sedangkan nilai 255 menjamin sebuah router pasti akan menjadi DR. Router ID biasanya akan menjadi sebuah "tie breaker" jika nilai Priority-nya sama. Jika

dua buah router memiliki nilai Priority yang sama, maka yang menjadi DR dan BDR adalah router dengan nilai router ID tertinggi dalam jaringan.

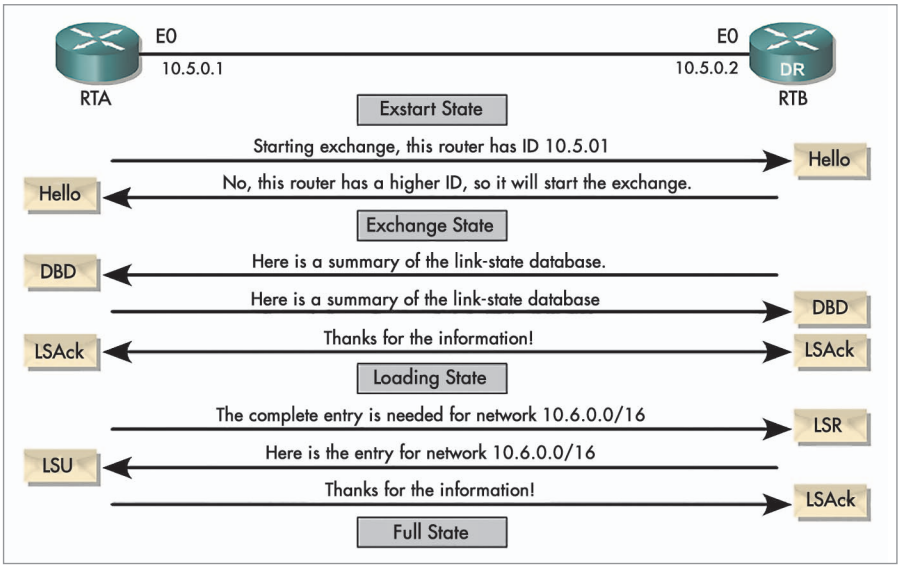
Setelah DR dan BDR terpilih, langkah selanjutnya adalah mengumpulkan seluruh informasi jalur dalam jaringan.

3. Mengumpulkan State-state dalam Jaringan

Setelah terbentuk hubungan antar-router-router OSPF, kini saatnya untuk bertukar informasi mengenai *state-state* dan jalur-jalur yang ada dalam jaringan. Pada jaringan yang menggunakan media broadcast multiaccess, DR-lah yang akan melayani setiap router yang ingin bertukar informasi OSPF dengannya. DR akan memulai lebih dulu proses pengiriman ini. Namun yang menjadi pertanyaan selanjutnya adalah, siapakah yang memulai lebih dulu pengiriman data

Terminologi dalam OSPF.

TERMINOLOGI	DESKRIPSI
Adjacency	Status yang terbentuk ketika dua buah router yang saling bertetangga telah bertukar informasi routing dan telah memiliki tabel topologi yang sama. Database mereka akan saling disinkronisasi dan mereka pasti akan memiliki database yang sama
Area	Sebuah group dari banyak router yang berada dalam satu area ID. Setiap router yang ada dalam satu area memiliki topologi table yang sama. Setiap router yang ada dalam satu area adalah internal router.
Back-up Designated Router (BDR)	Router yang bertugas sebagai back-up bagi router DR pada waktu router DR mengalami masalah.
Cost	Merupakan metrik dari OSPF. Router Cisco menggunakan inverse bandwidth sebagai cost-nya. Artinya semakin besar bandwidth, maka cost-nya semakin kecil dan semakin dipilih. Cost ini bisa diatur secara manual.
Database descriptor	Sering disebut juga dengan istilah Database Descriptor Packet (DDP) adalah sebuah paket yang membawa LSA yang mendeskripsikan link-link dari semua router yang ada dalam tabel topologi router tetangganya.
Designated router (DR)	Sebuah router yang bertanggung jawab untuk membangun adjacency dengan semua router yang ada dalam jaringan broadcast multiaccess seperti misalnya ethernet atau FDDI. DR akan memastikan semua router dalam jaringan tersebut memiliki database topologi yang sama.
Exchange state	State di mana kedua router tetangga menemukan pemetaan topologi jaringan. Ketika dua buah router menjadi adjacent, mereka pertama-tama harus saling bertukar DDP untuk memastikan mereka memiliki topologi yang sama.
Extart state	State di mana router tetangga memberikan informasi DDP secara sekuensial untuk membentuk hubungan master/slave antara kedua router ini.
Init state	State di mana sebuah paket hello telah dikirimkan keluar oleh sebuah router dan router dalam keadaan menunggu balasannya.
Internal router	Router yang memiliki interface yang semuanya berada dalam satu area yang sama.
Link-state advertisement (LSA)	Sebuah paket yang mendeskripsikan link beserta statusnya dari sebuah router. LSA memiliki beberapa tipe sesuai dengan status link yang diinformasikannya.
Link-state database	Lebih dikenal juga sebagai peta topologi. Database ini menyimpan pemetaan dari setiap router, link-link apa saja yang ada, dan status dari link tersebut. Di dalamnya juga terdapat pemetaan dari setiap segmen jaringan dan jalan-jalannya menuju ke sana.
Neighbour	Sebuah router yang berada dalam link yang sama yang mana akan saling bertukar informasi routing.
Neighbour table	Sebuah tabel yang dibangun dari pesan hello yang diterima dari router tetangga. Pesan hello ini juga membawa informasi list dari router-router tetangga lainnya.
Priority	Sebuah parameter buatan Cisco yang memungkinkan penggunanya mengatur secara manual prioritas router dalam pemilihan DR dan BDR.
SPF tree	Tree dari topologi jaringan. Tree ini dapat digambarkan setelah algoritma SPF dijalankan. Algoritma ini akan memangkas jalur-jalur yang ada dan hanya menyisakan jalur-jalur terbaik yang bebas looping dan yang terpendek menuju ke suatu lokasi.
Topology table	Topologi table adalah sebuah database jaringan yang menyimpan semua data mengenai link-link yang ada pada seluruh jaringan.



Dengan melewati beberapa fase yang cukup panjang, router OSPF akan mendapatkan rute-rute pilihan untuk menuju ke suatu lokasi.

link-state OSPF tersebut pada jaringan Point-to-Point?

Untuk itu, ada sebuah fase yang menangani siapa yang lebih dulu melakukan pengiriman. Fase ini akan memilih siapa yang akan menjadi master dan siapa yang menjadi slave dalam proses pengiriman. Router yang menjadi master akan melakukan pengiriman lebih dahulu, sedangkan router slave akan mendengarkan lebih dulu. Fase ini disebut dengan istilah *Exstart State*.

Router master dan slave dipilih berdasarkan router ID tertinggi dari salah satu router. Ketika sebuah router mengirimkan Hello packet, router ID masing-masing juga dikirimkan ke router neighbour. Setelah membandingkan dengan miliknya dan ternyata lebih rendah, maka router tersebut akan segera terpilih menjadi master dan melakukan pengiriman lebih dulu ke router slave.

Setelah fase Exstart lewat, maka router akan memasuki fase *Exchange*. Pada fase ini kedua buah router akan saling mengirimkan *Database Description Packet*. Isi paket ini adalah ringkasan status untuk seluruh media yang ada dalam jaringan. Jika router penerimanya belum memiliki informasi yang ada dalam paket Database Description, maka router pengirim akan masuk dalam fase loading state. Fase loading state merupakan fase di mana sebuah router mulai mengirimkan informasi state secara lengkap ke router tetangganya.

Setelah loading state selesai, maka router-router yang tergabung dalam OSPF akan memiliki informasi state yang lengkap dan penuh dalam database statenya. Fase ini disebut dengan istilah *Full state*. Sampai fase ini proses awal OSPF sudah selesai, namun database state tidak bisa digunakan untuk proses *forwarding* data. Maka dari itu, router akan memasuki langkah selanjutnya, yaitu memilih rute-rute terbaik menuju ke suatu lokasi yang ada dalam database state tersebut.

4. Memilih Rute Terbaik untuk Digunakan

Setelah informasi seluruh jaringan berada dalam database, maka kini saatnya untuk memilih rute terbaik untuk dimasukkan ke dalam routing table. Jika sebuah rute telah masuk ke dalam routing table, maka rute tersebut akan terus digunakan. Untuk memilih rute-rute terbaik, parameter yang digunakan oleh OSPF adalah Cost. Metrik Cost biasanya akan menggambarkan seberapa dekat dan cepatnya sebuah rute. Nilai Cost didapat dari perhitungan dengan rumus:

$$\text{Cost of the link} = 10^8 / \text{Bandwidth}$$

Router OSPF akan menghitung semua cost yang ada dan akan menjalankan algoritma *Shortest Path First* untuk memilih rute terbaiknya. Setelah selesai, maka rute tersebut langsung dimasukkan dalam routing table dan siap digunakan untuk forwarding data.

5. Menjaga Informasi Routing Tetap Up-to-date

Ketika sebuah rute sudah masuk ke dalam routing table, router tersebut harus juga me-*maintain state* database-nya. Hal ini bertujuan kalau ada sebuah rute yang sudah tidak valid, maka router harus tahu dan tidak boleh lagi menggunakannya. Ketika ada perubahan link-state dalam jaringan, OSPF router akan melakukan *flooding* terhadap perubahan ini. Tujuannya adalah agar seluruh router dalam jaringan mengetahui perubahan tersebut.

Sampai di sini semua proses OSPF akan terus berulang-ulang. Mekanisme seperti ini membuat informasi rute-rute yang ada dalam jaringan terdistribusi dengan baik, terpilih dengan baik dan dapat digunakan dengan baik pula.

Jaringan Besar? Gunakan OSPF!

Sampai di sini proses dasar yang terjadi dalam OSPF sudah lebih dipahami, meskipun masih sangat dasar dan belum detail. Melihat proses terjadinya pertukaran informasi di atas, mungkin Anda bisa memprediksi bahwa OSPF merupakan sebuah routing protokol yang kompleks dan rumit. Namun di balik kerumitannya tersebut ada sebuah kehebatan yang luar biasa. Seluruh informasi state yang ditampung dapat membuat rute terbaik pasti terpilih dengan benar. Selain itu dengan konsep hirarki, Anda dapat membatasi ukuran link-state database-nya, sehingga tidak terlalu besar. Artinya proses CPU juga menjadi lebih ringan.

Pada edisi selanjutnya, akan dibahas mengenai bagaimana sistem area yang ada dalam OSPF dan pernak-pernik apa saja yang ada dalam implementasinya. Selamat belajar! ■

LEBIH LANJUT

http://www.cisco.com/en/US/tech/tk365/technologies_q_and_a_item09186a0080094704.shtml

➔ Pada situs ini, Anda akan mendapatkan FAQ OSPF lengkap dengan *command* implementasinya.

Lebih baik membeli PSU dengan *power* yang hanya cukup dengan kualitas terbaik, dari pada membeli PSU yang berkekuatan sangat besar (berlebihan) dengan kualitas biasa saja. Ungkapan ini dapat menjadi petunjuk bagi Anda yang baru akan membeli *power supply unit* atau yang biasa disebut PSU.

Fadilla Mutiarawati

PSU, Bagian Terpenting yang Sering Diabaikan

"Motheboard apa yang akan dipakai? Berapa kecepatan processor yang akan digunakan? Berapa besar harddisk yang diinginkan? Bagaimana dengan memorynya? Jenis VGA apa yang akan dipilih?"

"Apakah akan menggunakan CD drive, DVD drive, CD-RW drive atau bahkan DVD-RW drive? Mau pakai keyboard-mouse optical, wireless, atau wireless optical?" ini adalah pertanyaan umum yang muncul dalam benak seseorang yang akan membeli sebuah komputer. Rasanya pertimbangan dalam menggunakan atau memilih power supply tidak menjadi sesuatu yang penting atau dominan, bahkan sebagian besar masyarakat lebih tidak peduli tentang power supply yang akan dibelinya, dan menyerahkan pilihan pada pemilik toko.

Hal ini memang sangat ironis, mengingat tanpa power supply komputer tidak mungkin dapat dijalankan. Menggunakan power supply yang tidak tepat saja dapat mengakibatkan kegagalan sistem yang tidak jarang memberikan efek kepada komponen lain. Contohnya saja jika *over heat* dialami oleh DVD-RW drive Anda, hal ini kemungkinan power supply dapat menjadi penyebabnya. Oleh sebab itu, ada baiknya dalam membeli sebuah komputer jangan lupa untuk ikut mempertimbangkan power supply yang akan digunakan.

Ada dua ungkapan yang paling terkenal berkaitan dengan power supply. Yang pertama adalah semakin berat bobot power supply, maka akan semakin baik harganya.

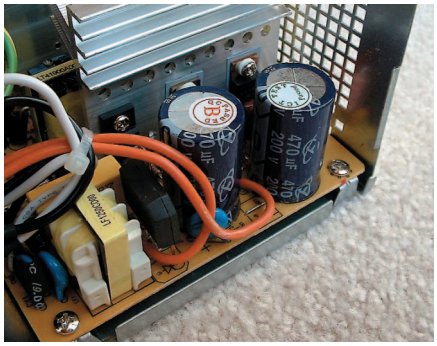
Sedangkan kalimat yang kedua adalah lebih baik membeli power supply dengan kekuatan yang cukup, namun dengan kualitas yang sangat baik atau bahkan yang terbaik. Daripada membeli power supply dengan kekuatan yang sangat berlebihan dengan kualitas biasa saja atau harga yang murah.

Standar PSU

Dalam menjalankan fungsinya memberikan tenaga pada komponen-komponen komputer, power supply juga memberikan dampak-dampak lain. Satu hal yang paling dominan adalah power supply juga menentukan *casing* yang akan digunakan. Atau sebaliknya casing juga akan menentukan power supply yang akan digunakan.

Dalam kaitannya dengan casing yang akan digunakan, power supply memiliki berbagai macam standar. Standar ini akan mempengaruhi beberapa faktor kecil. seperti bentuk power supply dan casing. Atau jumlah komponen yang memang secara langsung menggunakan komputer. Standar juga mempengaruhi sistem *switching* serta besarnya tenaga yang dihasilkan.

Standar juga akan mempengaruhi konektor yang tersedia pada power supply tersebut. Contoh saja standar baru ATX 12V 2.0. Pada standar ini ada beberapa perubahan pin utama yang pada ATX sebelumnya 20 pin, pada standar baru terdapat 24 pin. Jika pada standar sebelumnya dibutuhkan SATA adapter, pada standar yang baru konektor



Komponen dalam yang berkualitas biasanya akan menambah bobot PSU.

Semakin besar CFM, *fan* semakin baik.

SATA sudah disediakan langsung dari PSU. Konektor SATA ini disediakan baik secara langsung atapun dari cabang.

Lain lagi halnya dengan komputer Dell yang memiliki standar tersendiri untuk PSU, salah satu yang sangat signifikan dari standar Dell ini adalah pin utamanya yang memiliki jumlah pin 16 buah. Berbeda dengan ATX yang berjumlah 20 pin. Oleh sebab itu dalam membeli PSU, tidak hanya casing yang mempengaruhi motherboard juga ikut mempengaruhi. Sebab pin utama akan terhubung langsung ke motherboard.

Selain menentukan bentuk casing, dalam kerjanya power supply juga beberikan hal selain tenaga yaitu suara. Jika Anda tidak tepat memilih power supply atau tidak mendapatkan power supply yang tepat, maka Anda pun akan diganggu oleh suara yang ditimbulkan power supply komputer tersebut.

Konektor

Jika akan membeli sebuah PSU, hal lain yang tidak kalah penting adalah mengetahui keberadaan konektor-konektor penting dibawah ini. Sebab konektor-konektor ini adalah yang menghubungkan PSU dengan komponen-komponen komputer nantinya.

Konektor Motherboard (Konektor Utama)

Bentuknya sangat panjang. Dapat dikatakan sebagai konektor paling panjang. Konektor ini akan terhubung ke motherboard. Masing-masing standar memiliki panjang pin yang berbeda-beda. Contohnya yang sudah disebutkan tadi, yaitu Dell dan ATX12V 2.0 yang masing-masing menggunakan 24 pin dan 16 pin. Sedangkan ATX 1.3 yang lebih umum digunakan saat ini menggunakan 20 pin. Jumlah pin yang akan digunakan tergantung pada motherboard yang Anda pasang.

Konektor Processor Pentium 4

Konektor processor digunakan untuk memberikan daya bagi processor agar dapat bekerja. Konektor ini bentuknya sangat kecil terdiri dari empat pin tersusun dua baris. Konektor ini menyalurkan tegangan 12V.

Biasanya motherboard yang dipergunakan untuk processor berkecepatan sangat tinggi seperti Pentium 4 2,8 GHz memiliki konektor tersebut.

Konektor IDE

Ini adalah konektor yang digunakan untuk menyalurkan daya pada harddisk dan CD/DVD-ROM. Konektor ini terdiri dari empat pin. Dan biasanya tersedia sebanyak empat buah untuk setiap PSU. Namun jika ternyata kebutuhan akan konektor ini lebih banyak, maka Anda dapat menggunakan Splitter Y. Setiap satu splitter ini akan membelah sebuah konektor IDE menjadi dua buah konektor IDE. Atau bagi Anda yang akan menggunakan harddisk SATA, maka dapat menggunakan SATA Adapter yang akan mengubah konektor IDE menjadi konektor SATA. Namun, hal ini tidak perlu dilakukan bila Anda menggunakan PSU ATX12V 2.0 yang baru.

Konektor Floopy

Keberadaan floopy dalam sebuah komputer belakangan ini memang hampir dilupakan. Namun bukan berarti tidak lagi di-*support* oleh power supply. Semua power supply pasti akan menyediakan konektor floopy. Sebab tidak hanya floopy drive saja yang akan menggunakan konektor ini. Perangkat media lain seperti card reader internal umumnya juga menggunakan konektor floopy untuk mengambil sumber daya dari PSU.

Konektor AUX

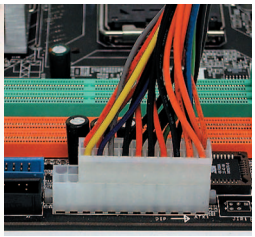
Satu lagi tambahan adalah konektor AUX, bentuknya terdiri dari enam pin yang tersusun sebaris. Bila motherboard Anda memiliki konektor ini, mengapa tidak Anda juga membeli PSU yang dapat men-*support*-nya.

Watt yang Tepat

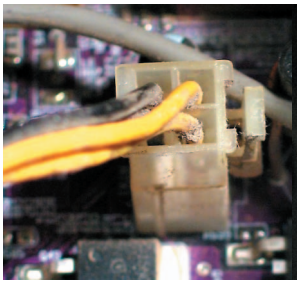
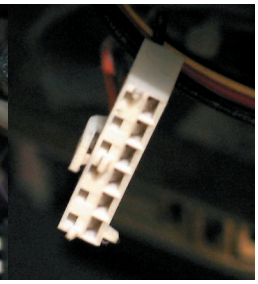
Untuk dapat bekerja, setiap komponen dalam komputer membutuhkan asupan tenaga yang konstan. Meskipun listrik di rumah Anda tidak stabil, namun power

Tabel Kebutuhan Daya Setiap Komponen.

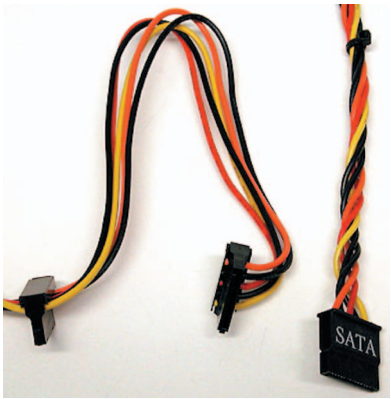
COMPONENT	REQUIREMENT	LINE(S) USED
AGP Video Card	30 - 50W	+3,3V
Average PCI Card	5 - 10W	+5 V
10/100 NIC	4W	+3,3V
SCSI Controller PCI Card	20W	+3,3V and +5V
Floppy Drive	5W	+5V
CD-ROM	10 - 25W	+5V and +12V
DVD-ROM	10 - 25W	+5V and +12V
CD-RW	10 - 25W	+5V and +12V
7200 rpm IDE Hard Drive	5 - 20W	+5V and +12V
10,000rpm SCSI Drive	10 - 40W	+5V and +12V
Case/CPU Fans	3W (ea.)	+12V
Motherboard (w/o CPU or RAM)	25 - 40W	+3.3V and +5V
RAM	8W per 128MB	+3,3V
Pentium III Processor	38W	+5V
Pentium 4 Processor	70W	+12V
AMD Athlon Processor	70W	+12V

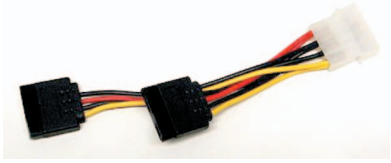


Konektor motherboard ATX 20pin dan ATX 24pin.

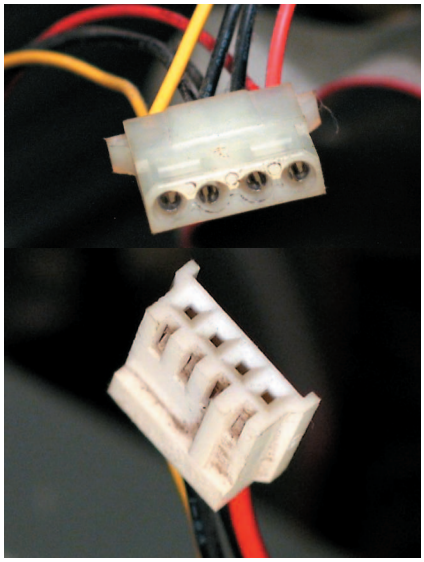



Konektor untuk processor Pentium 4 dan AUX.





Konektor SATA pada ATX12V 2.0 dan Adapter SATA.



Konektor IDE dan Floopy.

supply akan mencoba untuk melakukan hal tersebut secara terus menerus sampai Anda selesai membutuhkannya.

Oleh sebab itu, bagi Anda yang memiliki listrik rumah naik turun, sangat disarankan untuk menggunakan *stabilizer* listrik yang baik untuk komputer Anda. Hal ini sangat membantu kerja power supply untuk tetap memberikan tenaga yang konstan.

Umumnya setiap power supply memiliki beberapa konektor yang masing-masing memiliki nilai 3,3 Volt, 5 Volt, dan 12 Volt. 3,3 Volt dan 5 Volt ditujukan untuk komponen-komponen yang tidak memiliki motor atau sesuatu yang tidak bergerak seperti chipset, PCI Card, dan sebagainya. Dan 12 Volt ditujukan untuk komponen-komponen yang menggunakan motor seperti harddisk, CD drive, dan sebagainya.

Sedangkan watt dari masing-masing komponen berbeda-beda hal ini karena ampere yang dibutuhkan untuk setiap komponen juga berbeda. Jika ingin mengetahui seberapa besar watt yang dibutuhkan oleh komputer Anda, maka Anda dapat menghitungnya terlebih dahulu dengan bantuan tabel yang telah kami sediakan. Jumlahkan semua kebutuhan watt tersebut, maka itulah nilai yang dibutuhkan oleh komputer Anda.

Namun, janganlah Anda membeli power supply dengan nilai watt yang sama dengan yang baru saja Anda hitung, sebab ini akan membuat power supply dipaksa untuk bekerja maksimal sekali. Sebagai dampaknya akan mengakibatkan power supply *over heat* dan rusak lebih cepat.

Selain itu, ada baiknya juga jika Anda menyisihkan beberapa watt untuk keperluan tambahan seperti upgrade (misalnya penambahkan drive atau kartu tambahan) atau mungkin perangkat lain seperti kipas, lampu dan sebagainya. Kebutuhan-kebutuhan tersebut tentu akan memerlukan daya juga. Selain daya kebutuhan-kebutuhan tersebut, tentu akan memerlukan juga pin dari power supply oleh sebab itu perhatikan jumlah pin. Apakah sekiranya mencukupi atau tidak untuk keperluan upgrade ke depannya.

Selain nilai watt, perhatikanlah pin yang disediakan. Jika Anda menggunakan komputer dengan Pentium 4 atau AMD Athlon, voltase yang digunakan agak sedikit berbeda. Sebab Pentium 4 atau AMD Athlon dan processor-processor terbaru saat ini menggunakan voltase 12Volt. Sedangkan Pentium III menggunakan 5 Volt.

Berat, Lebih Baik

Salah satu cara yang termudah mengetahui bagaimana memilih power supply yang baik adalah dari beratnya. Pada nilai watt yang sama bobot yang semakin berat artinya semakin baik.

Mengapa dari bobot? Sebab bobot yang semakin berat menandakan bahwa komponen di dalamnya lebih besar. Lebih besar kapasitornya, lebih besar *heatsink*, dan lebih banyak kipasnya.

Kapasitor menjadi bagian utama untuk power supply dalam menghasilkan daya yang dibutuhkan. Sedangkan heatsink dan kipas sangat berguna dalam membuang panas untuk menghindari terjadinya *over heat*.

Berkaitan dengan kipas, ada power supply yang dilengkapi dengan *fan control* yang berfungsi untuk mengatur kipas. Fan control yang ditawarkan ada dua jenis, manual dan otomatis. Untuk fan control otomatis, maka kipas akan berputar sesuai dengan yang dibutuhkan saja. Perubahan putaran kipas akan berjalan secara otomatis tergantung pada deteksi yang dilakukan oleh power supply itu sendiri.

Catatan lain tentang kipas adalah nilai CFM (*cubic feet perminute*). Nilai ini mewakilkan berapa banyak udara yang dapat diputar oleh fan. Semakin tinggi semakin baik.

Listrik berperan penting dalam sistem komputer Anda, memperhatikannya dapat memberikan umur lebih panjang pada komputer. Karena itu, tidak ada salahnya jika akan mengganti atau membeli perangkat baru Anda ikut mempertimbangkannya. Bukankah mencegah lebih baik daripada mengobati. Jangan tunggu komputer Anda rusak. Segeralah perhatikan PSU yang Anda gunakan! ■

LEBIH LANJUT

www.atxpowersupplies.com
➔Ini merupakan alamat situs web tentang power supply.

Dalam memilih MP3, sebaiknya Anda memperhatikan tidak hanya format dan kemampuan MP3-nya saja atau tergiur dengan kapasitas yang besar. Sebab kapasitas yang besar biasanya menggunakan bahan yang tidak fleksibel untuk dibawa bergerak.

Fadilla Mutiarawati

Memilih MP3 Player yang Sesuai

▶Jangan terburu tergiur dengan kapasitas besar harga murah, sebab belum tentu yang berkapasitas dan besar sesuai dengan harapan Anda. Dalam membeli MP3 Player kapasitas bukan satu-satunya parameter yang perlu diperhatikan masih banyak hal lain yang tidak boleh luput.

Semakin hari popularitas MP3 Player semakin menanjak. Perlahan-lahan makin banyak konsumen yang lebih tertarik untuk membeli MP3 Player ketimbang Walkman, DiscMan, atau CD Player. Hal ini tidak hanya disebabkan kapasitas saja, namun semakin hari harga lagu MP3 memang semakin murah. Meskipun dari segi kualitas CD audio masih lebih baik ketimbang MP3, masyarakat awam tidak mempedulikan. Sebab perbedaannya memang tidak terlalu signifikan.

Philips Nike MP3Run adalah sala satu *player* yang menggunakan *flash drive*.

Salah satu yang sangat berperan dalam perkembangan teknologi MP3 Player adalah media penyimpanan MP3 itu sendiri. Media-media ini tidak berbeda dengan media-media yang digunakan untuk menyimpan data pada umumnya. Namun, kita ketahui sendiri bahwa saat ini perkembangan media penyimpanan memang telah berkembang dengan sangat pesat. Mulai dari munculnya flash disk, DVD, sampai akhirnya ada yang disebut Blue Ray.

Dulu untuk memainkan lagu MP3, media yang digunakan hanyalah CD. Sekarang tidak hanya CD. Banyak media lain yang ikut menjadi bagian. Dan media ini menjadi salah satu parameter yang ikut menentukan baik harga, kapasitas, dan fleksibilitas MP3 Player itu sendiri.

Selain media penyimpanan, hal lain yang tidak kalah jarangnya dipertimbangkan adalah kemampuan. Apa saja yang dapat dilakukan oleh MP3 Player selain dapat memperdengarkan lagu. Selain fitur tambahan format juga dapat memegang peranan penting.

Pada artikel ini, Anda dapat mempelajari apa saja yang menjadi bagian-bagian penting dalam MP3 Player. Sehingga bila nanti Anda akan membelinya, barang yang dibelikan sesuai dengan yang dibutuhkan.

Hard Drive

Salah satu bagian dari MP3 Player yang paling dominan adalah media penyimpanannya. Untuk bagian ini, Anda harus lebih teliti membelinya. Sebab mobilitas MP3 Player salah satunya ditentukan dari jenis media penyimpanan yang digunakannya.

Ada empat jenis dari media penyimpanan yang digunakan pada MP3 Player. Masing-masing jenis selain akan mempengaruhi bentuk/ukuran/bobot juga akan mempengaruhi kapasitas dan harga tentunya.

Media yang paling besar ruang penyimpanannya adalah hard drive. MP3 player yang menggunakan hard drive sebagai medianya, ditawarkan dengan kapasitas dari 10 GB sampai 60 GB.

Salah satu pemain yang sangat do-

iPod Photo adalah salah stau player yang menggunakan hard drive.

minan adalah iPod dari Apple. hard drive berukuran 1,8 inci ini sanggup menyimpan lebih dari 17000 file MP3 (dengan bobot rata-rata setiap file 3,5 MB). Namun berhubung hard drive merupakan media yang bekerja secara mekanik, maka hal ini membatasi si pengguna dalam bergerak. Sebab goncangan yang terlalu kencang dapat mengakibatkan gangguan kerja hard drive tersebut. Atau bahkan jika terlalu dramatis dapat menyebabkan kerusakan pada hard drive.

Meskipun demikian, bila Anda tergolong seseorang yang tidak terlalu banyak memiliki aktivitas pada saat mendengarkan MP3, maka player dengan media hard drive dapat dijadikan pilihan. Selain kapasitas yang jadi bahan pertimbangan, harga pun memiliki peranan yang cukup diperhitungkan. Untuk harga setiap 1 GB dengan media hard drive dapat mencapai hanya ±US$5 saja. Sedangkan bila dibandingkan dengan flash disk dapat mencapai US$150-US$200.

Micro Hard Drive

Media penyimpanan lain yang dapat dianggap lebih ringkas dan ringan dari hard drive adalah micro hard drive atau dapat juga dikatakan hard drive mini. Sesuai dengan namanya, hard drive yang digunakan oleh MP3 ini berukuran sangat kecil, lebih kecil ketimbang hard drive yang disebutkan sebelumnya. Ukuran diameter micro hard drive adalah 1 inci, 0,8 inci lebih kecil dibandingkan hard drive pada MP3 sebelumnya.

Lebih kecilnya media penyimpanan yang digunakan oleh MP3 Player ini membuat keseluruhan ukuran MP3 juga lebih kecil ketimbang yang menggunakan hard drive sebelumnya. Tapi sayangnya, ukuran fisik juga mempengaruhi kapasitas yang dapat ditampungnya. Banyaknya file yang dapat ditampung oleh micro hard drive saat ini baru mencapai 1,5 GB sampai 6 GB saja.

Dikarenakan komponen dan cara kerjanya sangat mirip dengan hard drive, maka micro hard drive juga menggunakan sistem mekanik, sehingga pada saat bekerja akan ada bagian-bagian yang berputar dengan sangat cepat seperti layaknya sebuah hard drive.

Kemiripan lain dari kedua player ini adalah sumber tenaga yang digunakan. Kedua player umunya menggunakan baterai *rechargeable*. Baterai yang digunakan ada yang dipasangkan secara *built-in* ada juga yang tidak. Bagi yang membeli MP3 Player dengan baterai built-in, jika ada masalah dengan baterai atau masa baterai telah habis tentu akan lebih merepotkan ketimbang dengan baterai yang bukan built-in. Meskipun demikian, biasanya baterai built-in memiliki kelebihan daya dukung yang lebih lama ketimbang baterai biasa.

MP3 Player dengan media micro hard drive dapat menjadi pilihan bagi mereka yang memiliki dana terbatas untuk membeli MP3 player yang menggunakan hard drive. Dari segi harga player ini masih lebih mahal ketimbang hard drive namun jauh lebih murah ketimbang Flash Drive. Untuk 1 GB-nya micro hard drive mencapai US$25-US$30.

Flash Drive

Yang termasuk kelompok paling fleksibel dan tentu saja lebih mahal harga per 1 MB-nya adalah MP3 yang menggunakan media flash drive. MP3 Player dengan media ini dikatakan paling fleksibel dikarenakan bentuk dan sistem kerja media itu sendiri. Flash drive bukan merupakan media penyimpanan yang bersifat mekanik, flash drive dikatakan juga sebagai *solid state media*. Artinya, pada proses kerjanya tidak ada satupun bagian yang bergerak dalam flash drive. Di samping itu, secara fisik flash drive memiliki ukuran dan bobot yang kecil dan ringan. Untuk perbandingannya, perhatikan saja ukuran USB disk atau flash memory lain yang digunakan perangkat *mobile* Anda.

Sistem kerja dan ukuran/bobot inilah yang membuat MP3 dengan flash drive sangat mungil dan ringan. Yang menjadi konsekuensi media flash drive tak lain adalah kapasitas. Sampai artikel ini diturunkan, kapasitas yang terbesar dari MP3 player flash drive adalah 2 GB saja. Sangat jauh berbeda dari yang menggunakan hard drive atau micro hard drive.

Untuk mengoperasikan MP3 Player bermedia flash drive tidak terlalu memerlukan tenaga yang besar, oleh sebab itu biasanya MP3 Player ini menggunakan tenaga dari dua baterai AA atau AAA.

MP3 Player flash drive sangat cocok bagi mereka yang gemar mendengar musik sambil berolahraga. Bahkan ada juga beberapa MP3 Player flash drive yang didesain tahan air (*water resistant*), sehingga dapat dipergunakan untuk olah raga *outdoor* yang lebih ektrim. Salah satu contoh produk MP3 Player flash drive yang tahan air adalah Philips Nike MP3Run dengan memory sebesar 256 MB.

CD

Media yang paling tua yang digunakan oleh MP3 Player adalah CD. Saat ini sudah semakin umum di pasaran yang menawarkan DiscMan yang sudah dilengkapi dengan MP3 Player. Sehingga Anda tidak hanya dapat menikmati lagu dengan kualitas CD saja, melainkan juga MP3 sekaligus. Ini tergolong player yang sangat murah. Hanya saja ukurannya

DiscMan dari Panasonic yang juga dapat menjalankan CD MP3.

Nomad Zen Micro, MP3 Player yang menggunakan micro drive.

masih tergolong besar dan dianggap kurang fleksibel untuk data yang besar. Kemampuannya pun biasanya tidak selengkap MP3 jenis yang lain. Atau konektibilitas dengan komputer agak terbatas.

Namun dari segi harga player ini tergolong sangat murah, apalagi dengan harga CD yang semakin lama semakin murah. Untuk player-nya tersedia dari harga Rp300 ribu sampai lebih dari Rp1 juta. Dan harga CD-nya hanya Rp2 ribu per keping. Kapasitasnya dapat mencapai 700 MB setiap CD. Sangat murah, bukan?

Display

Komponen lain yang ikut melengkapi sebuah *player* adalah *display*. Ada berbagai macam display ditawarkan. Mulai yang berukuran kecil sampai seukuran kartu nama. Display ini juga hadir dengan bermacam jenis dan resolusi. Ada yang hanya mampu menampilkan warna hitam saja. Ada pula yang mampu menampilkan foto dengan resolusi yang cukup baik. Seberapa jauh kebutuhan Anda akan display tergantung pada kapasitas dan penggunaannya.

Bagi yang ingin memanfaatkan MP3 player hanya sebagai player saja dan kapasitas tidak terlalu besar (<1 GB) tidak ada salahnya hanya tidak menggunakan display atau hanya menggunakan display satu baris.

Sedangkan bagi yang akan membeli MP3 Player dengan media yang sangat besar, maka layar dapat menjadi alat bantu melihat isi player. Apalagi jika player juga digunakan untuk kebutuhan lain, seperti merekam lagu atau sekaligus tempat menyimpan data.

Seperti layaknya sebuah ponsel, kualitas layar pada MP3 Player dapat dilihat dari jenis dan resolusinya. Dan satu hal yang perlu Anda ingat bahwa semakin tinggi resolusi sebuah display atau layar akan sangat mempengaruhi daya tahan baterai. Sebab semakin tinggi resolusi sebuah display, biasanya akan membutuhkan tenaga lebih besar juga. Misalnya sebuah player yang menggunakan layar berwarna seperti iPod Photo, akan memerlukan daya batere yang lebih banyak ketimbang iPod Shuffle yang hanya menggunakan layar kecil sederhana.

Baterai

Baterai adalah sumber tenaga yang digunakan oleh semua MP3 Player. Berapa lama sebuah player dapat tetap menyala tergantung pada jenis baterai yang digunakan.

Bagi Anda yang akan membeli sebuah player dengan media Flash atau CD, ada baiknya jika menggunakan baterai yang dapat di-*recharge*. Selain lebih efisien, daya tahannya pun dapat lebih lama. Meskipun hanya sekadar baterai AA atau AAA.

Sedangkan bagi Anda yang akan membeli player dengan media hard drive atau micro hard drive, masalah baterai dapat sedikit lebih rumit. Selain waktu *charging* yang lumayan lama (8-20 jam), umumnya baterai diletakkan secara *built-in*, sehingga sulit untuk diganti secara mandiri atau bahkan kadang Anda harus membeli yang baru jika baterai sudah tidak berfungsi lagi. Namun, ada juga player jenis ini yang menawarkan baterai yang fleksibel seperti Creative Nomad Jukebox Zen Xtra, yang baterainya dapat Anda ganti sendiri dengan mudah. Walaupun demikian mudahnya mengganti baterai tetap saja harga baterainya juga akan lebih mahal ketimbang baterai biasa.

Sebagai catatan saja, tidak ada salahnya jika sebelum membeli Anda bertanya terlebih dahulu, apakah mungkin mengganti baterai jika rusak atau tidak. Jika ya, hal ini tentu akan lebih menguntungkan.

Mana yang lebih lama men-support apakah baterai biasa atau baterai khusus? Sebenarnya baterai khusus memang lebih tahan lama dan memberikan dukungan yang lebih besar. Namun dukungan ini sendiri memang harus dilakukan, mengingat kebutuhan daya yang lebih besar dari player-player seperti hard drive maupun micro hard

CARA KERJA MP3 PLAYER

Apa yang dimiliki oleh sebuah MP3 Player sama dengan apa yang dimiliki oleh sebuah sound card. Hanya saja MP3 Player memiliki keterbatasan tertentu yang tidak dapat diubah. Sehingga aplikasi maupun format audio yang dimainkan oleh MP3 Player tidak seluas aplikasi atau format yang dapat dimainkan oleh komputer yang menggunakan sound card. Tetapi yang pasti setiap MP3 Player dapat memainkan file MP3.

Dalam sebuah MP3 Player ada beberapa komponen yang sangat penting. Dua di antaranya adalah *codec*, *firmware*, serta *converter*. Converter tugasnya adalah mengonversi data digital menjadi analog atau sebaliknya mengonversi sinyal analog menjadi data digital yang terdiri dari bilangan satu dan nol saja. Sedangkan codec adalah sebuah algoritma yang digunakan untuk mengompresi maupun dekompresi file oleh converter itu sendiri.

Pada sebuah MP3 Player yang paling sederhana setidaknya terdapat satu converter, yaitu mengonversi data digital menjadi analog dengan sebuah codec serta sebuah software atau firmware yang mengaplikasikan codec pada converter. Player yang paling sederhana ini hanya mampu memainkan file dengan satu format saja yaitu MP3, tanpa dapat melakukan aplikasi lain. Sedangkan player yang mampu melakukan beberapa hal sekaligus. Misalnya merekam suara juga, maka di dalamnya terdapat tambahan converter yang bertugas untuk mengonversi sinyal analog menjadi digital. Bila player yang Anda miliki dapat memainkan lebih dari satu format itu tandanya player tersebut memiliki lebih dari satu codec.

www.napster.com adalah salah satu situs men-*download* MP3.

drive. Oleh sebab itu selain bertanya tentang kemungkinan mengganti baterai, ada baiknya Anda mencari tahu juga berapa lama baterai dapat digunakan setelah di-charge penuh.

Computer ⇔ MP3 Player

Bila Anda akan membeli sebuah MP3 Player yang menggunakan media hard drive, micro hard drive, atau flash drive, kompatibilitas dengan komputer sangat perlu untuk diperhatikan. Sebab biar bagaimanapun, melalui komputerlah nantinya data Anda dapat ditransmisikan dengan lebih cepat. Dengan komputer jugalah di kemudian hari data—baca: file MP3—Anda dapat diproses lebih lanjut.

Sebenarnya ada tiga kompatibilitas yang harus diperiksa ketika akan membeli MP3 Player. Yang pertama adalah koneksi dengan komputer, *software* yang digunakan serta format yang mampu dimainkan.

● Koneksi

Apa yang digunakan oleh MP3 Player sebagai penghubung dengan komputer? Yang sangat umum saat ini adalah USB. Namun, ada juga player yang dilengkapi dengan firewire. Sebelum membeli tidak ada salahnya jika Anda memperhatikan komputer yang sudah lebih dulu dimiliki. Jika terdapat fasilitas firewire, tidak ada salahnya jika membeli player yang menggunakan firewire contohnya iPod dengan Macintosh. Namun jika komputer Anda tidak memiliki firewire card, maka sebaiknya jangan membeli player yang hanya menggunakan firewire saja. Carilah player yang menggunakan konektor USB atau agar lebih lengkap carilah player yang memiliki keduanya.

● Software Audio

Jika *player* Anda memiliki kompatibilitas dengan software MP3 player yang dimiliki komputer Anda—baca: media player—maka komunikasi player dengan komputer dapat berjalan lebih mudah.

Anda dapat langsung memindahkan atau mengganti nama pada daftar lagu (*playlist*) MP3 Player Anda seiring Anda menggantinya dengan media player di komputer Anda. Contohnya saja iPod dengan iTunes. Biasanya keterangan tentang kompatilitas tersebut tercantum pada boks ataupun lembar/buku manual player.

● Format

Format yang sudah pasti dapat dimainkan oleh MP3 Player adalah MP3 itu sendiri. Namun, tidak menutup kemungkinan untuk player memainkan format lain. Dan keterangan format ini umumnya selalu diinformasikan, baik pada boks maupun manual book. Semakin luas format yang dimainkan, tentu saja akan semakin baik. Biasanya format ini juga bergantung kepada media player, sumber file, ataupun komputer yang digunakan. Contoh saja iPod, selain dapat memainkan file MP3 pasti dapat juga memainkan lagu yang berformat AAC. Setiap format memiliki karakteristik masing-masing.

Fitur Pelengkap

Selain dapat memperdengarkan file MP3, sebagai nilai tambah MP3 Player banyak dipersenjatai dengan berbagai macam fitur tambahan menarik beraneka ragam.

- **Radio:** Selain memperdengarkan file MP3, ada juga player yang dapat berfungsi sebagai radio (FM saja, atau FM/AM). Dan terkadang ada juga player yang dapat menyimpan memory gelombang favorit.
- **Mic:** Ada beberapa player yang juga dilengkapi dengan *voice recording* dengan menggunakan mikrofon. Penggunaan fitur ini juga akan menggunakan ruang media penyimpanan player.
- **Data Storage:** Ada juga player yang dapat digunakan sebagai media penyimpanan file digital lain selain audio, seperti layaknya USB Disk.
- **Recording:** Selain merekam dengan bantuan mikrofon, ada juga beberapa player yang memiliki kemampuan merekam atau bahkan mengonversi langsung suara yang masuk melalui *channel Line-In* yang disediakan. Channel Line-in seperti layaknya dalam sebuah sound card yang dapat dimanfaatkan untuk memasukkan suara dari sebuah CD player, mikrofon tambahan, atau sumber suara lain.
- **Kualitas suara:** Ada beberapa player yang menawarkan kualitas suara dengan *noise ratio* sampai 95 dB. Atau ada juga player yang menawarkan format sangat baik selain MP3. Format yang hampir setara dengan CD audio. ■

LEBIH LANJUT

www.mp3.com
➔Alamat ini berisi informasi tentang MP3 lengkap dengan formatnya.

Lebih murah, mudah, dan luas dari *bluetooth*. Namun, sebagai standar baru *ZigBee* bukan saingan bluetooth. Ia hadir untuk memudahkan Anda mengontrol listrik, peralatan rumah tangga, atau bahkan perangkat keamanan kantor yang sering merepotkan.

Fadilla Mutiarawati

Berkenalan dengan ZigBee

Pernahkah Anda terbangun malam-malam karena lupa mengunci pintu rumah atau mematikan televisi? Untuk jarak dekat saja, rasanya segan meninggalkan kasur dan terkantuk-kantuk menuju pintu depan. Apalagi jika jaraknya mencapai 10 meter.

Satu-satunya alat kontrol yang mungkin dapat teraih, paling-paling hanya *remote* AC atau TV kamar. Sedangkan TV luar pasti menggunakan remote yang berbeda begitu pula dengan pintu yang menggunakan sistem terpisah lainnya.

Oleh sebab itu, jika segan bangun tengah malam hanya untuk memastikan pintu terkunci atau listrik telah dipadamkan, maka saatnya Anda mulai melirik menggunakan ZigBee.

Dengan ZigBee, semua dapat Anda lakukan tanpa harus bangun dari kasur hangat nan empuk. Di samping itu, dengan ZigBee juga Anda tidak perlu mengoleksi 5 atau bahkan 10 remote sekaligus hanya dalam satu rumah saja. Cukup satu untuk semua. ZigBee atau 802.15.4 adalah standar yang baru saja diresmikan Mei 2003 lalu.

Sampai saat ini, sudah terdapat lebih dari 100 perusahaan elektronik yang mengembangkan perangkat berbasis ZigBee. Perusahaan-perusahaan besar seperti Mitsubishi, Motorola, Philips, dan Samsung sudah mulai mencoba mendesain produk yang akan digunakan pada ZigBee.

Dengan ZigBee, seseorang dapat bebas menambahkan atau mengurangi perangkat yang digunakan. Ada 6500 perangkat dapat terhubung dengan ZigBee, mulai dari alarm rumah, pintu, panel lampu, *home theater*, sampai jendela dapat dikontrol dengan ZigBee. Penyusunannya pun dapat dilakukan secara beragam.

Dalam pengoperasiannya, ZigBee hanya memerlukan energi yang sangat minim, sehingga jika menggunakan batu baterai biasa (AA atau AAA) remote ZigBee dapat bertahan sampai dua tahun lamanya.

Meskipun demikian sebagai standar nirkabel baru, ZigBee bukanlah saingan untuk 802.11 a/b/g yang sudah terlebih dahulu hadir.

ZigBee

Ada tiga frekuenci yang digunakan untuk ZigBee. Masing-masing frekuensi memiliki kecepatan (*data rate* berbeda-beda), yaitu 2,4 GHz dengan kecepatan sebesar 250 Kbps yang digunakan untuk di seluruh dunia, 868 MHz dengan kecepatan 40 Kbps untuk di Eropa, dan 915 MHz dengan kecepatan 20 Kbps untuk di Amerika. Sedangkan kecepatan dan jumlah channel masing-masing adalah satu channel (channel 0) untuk frekuensi 915 MHz, 10 channel (channel 1 sampai 10) untuk frekuensi 868 MHz, dan 16 channel (channel 11 sampai 26) untuk frekuensi 2,4 GHz.

Logo ZigBee.

Jarak yang mampu ditempuh oleh ZigBee tanpa *repeater* atau penguat sinyal adalah 10 meter sampai 30 meter. Bila menggunakan penguat sinyal dapat mencapai 100 meter.

Latency yang dimiliki oleh ZigBee juga terhitung sangat singkat, bahkan hampir tidak terasa tepatnya adalah hanya 30ms.

ZigBee sendiri dapat dirangkai dengan menggunakan topologi jaringan bervariasi, yaitu Star, Mesh (*Peer to Peer*), dan Cluster Tree (gabungan star dan mesh). Jumlah *node*s (perangkat) yang dapat terhubung dengan *local address* dalam satu jaringan ZigBee yang se-

derhana dapat mencapai 65000 perangkat lebih atau tepatnya 2^{16}. Bahkan untuk jaringan yang lebih luas dapat mencapai 2^{64}, cukup banyak bukan?

ZigBee juga dinilai cukup aman, sebab data yang akan terkirim akan dienkripsi dengan metode enkripsi 128-bit *Advanced Encryption Standard*.

Satu lagi yang menjadi ciri khas ZigBee adalah konsumsi daya yang sangat kecil. Hal ini dikarenakan kemampuan diam yang dimiliki oleh perangkat ZigBee ketika tidak digunakan. Sehingga pemakaian daya listrik dapat lebih hemat.

Personal Area Network

ZigBee hadir untuk keperluan yang jauh lebih sederhana dibanding standar nirkabel lain yang sudah lebih dulu digunakan. Yang dikatakan sederhana adalah paket data yang tidak terlalu besar dan dalam jarak yang juga tidak terlalu luas.

Oleh sebab itu, kehadiran ZigBee lebih ditujukan untuk mendukung jaringan yang paling sederhana, yaitu *Personal Area Network*.

Dalam Personal Area Network sendiri sudah terdapat dua pemain yang terlebih dahulu dikenal. Yang paling lama adalah *infrared* lalu yang kedua adalah *bluetooth*.

Untuk teknologi infrared sudah bukan menjadi barang asing, mengingat hampir semua barang elektronik yang menggunakan *remote* memanfaatkan teknologi ini. Namun sayangnya untuk menggunakan infrared, ada syarat yang cukup mengganggu. Anda harus mengarahkan remote secara berhadapan dengan produk yang akan dikontrol. Kelemahan yang dimiliki oleh teknologi yang memanfaatkan sinar infra merah ini membuat penggunaannya perlahan mulai tergantikan.

Salah satu kandidat yang menggantikan peranan infra merah pada jaringan Personal Area Network ini adalah bluetooth. Berbeda dengan infrared yang memanfaatkan sinar infra merah, bluetooth menggunakan gelombang radio. Sehingga dalam penggunaannya tidak perlu dilakukan secara berhadap-hadapan.

Namun berhubung sampai saat ini bluetooth masih memerlukan biaya yang besar, maka untuk keperluan kontrol perangkat elektronik, infra merah masih nomor satu.

Sedangkan ZigBee sebagai kandidat terakhir mencoba untuk menyempurnakan teknologi yang sudah lebih dulu hadir. Media yang digunakan oleh ZigBee adalah gelombang radio. Sehingga pengoperasiannya sama dengan bluetooth yang tidak perlu berhadap-hadapan. Tetapi di sisi lain, ZigBee tidak memerlukan biaya produksi dan pengoperasian yang besar. Layaknya merangkat dengan infrared, ZigBee pun dijalankan hanya dengan menggunakan baterai AA atau AAA biasa.

Meskipun demikian, bukan berarti ZigBee lebih baik dari bluetooth sebab ternyata ada beberapa segmen aplikasi bluetooth yang tidak mungkin dilakukan oleh ZigBee.

Bagaimana dengan infrared? Untuk keperluan kontrol di masa yang akan datang, ZigBee dapat saja menggantikan infrared.

ZigBee vs Bluetooth

Tadi sempat disinggung bahwa kehadiran ZigBee bukan untuk menggeser bluetooth justru untuk menutupi tempat yang tidak dapat atau lemah dilakukan oleh bluetooth.

Misalnya saja untuk remote, mouse, atau keyboard. Di mana besarnya data yang dikirimkan tidak terlalu besar. Serta penggunaan daya yang diharapkan lebih efisien. Secara keseluruhan, ada beberapa hal yang sangat membedakan antara ZigBee dengan bluetooth.

Data Rate

Yang paling mencolok antara keduanya adalah bobot pengiriman paket data. Jika bluetooth memiliki data rate sebesar 1 Mbps, ZigBee hanya 250 Kbps. Sehingga untuk aplikasi-aplikasi sederhana seperti remote yang sangat kecil, ZigBee lebih efisien. Sedangkan bluetooth yang memiliki kemampuan seperti layaknya 802.11 lebih cocok digunakan untuk keperluan-keperluan yang lebih rumit. Misalnya untuk transfer data audio (sebagai *handsfree*), gambar multimedia dalam presentasi atau antarponsel, atau koneksi Internet.

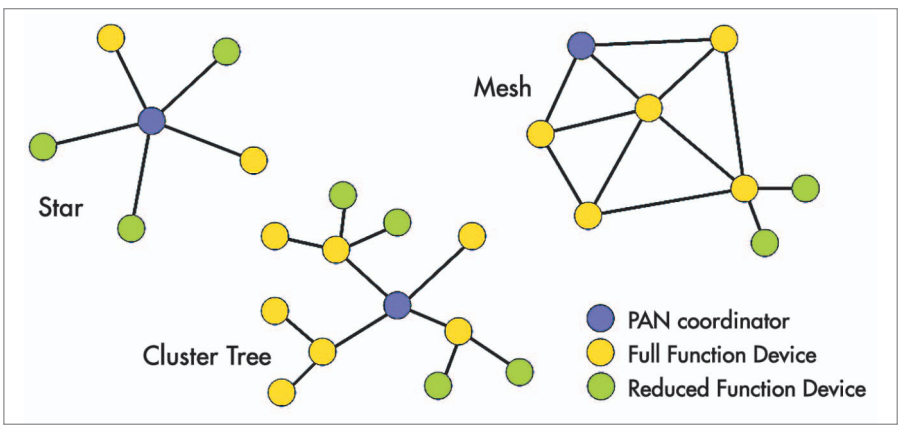
Oleh sebab itu, dari segi data rate saja sudah dapat dilihat bahwa keduanya berperan dalam dua lingkup kerja yang berbeda. ZigBee ditujukan untuk perangkat kontrol dan monitoring. Sedangkan bluetooth lebih sebagai pengganti kabel komunikasi untuk jaringan kecil yang membutuhkan data lebih besar.

Jumlah Nodes

Dalam satu jaringan bluetooth hanya ada 8 node yang dapat terhubung satu master dan 7 slave. Sedangkan pada zigbee ada lebih dari 6500 node yang dapat terhubung. Hanya saja jika pada bluetooth dapat berhubungan dengan jaringan lain (LAN, WAN, Internet) ZigBee tidak demikian halnya.

Latency

Waktu *latency* yang dimiliki oleh bluetooth dapat mencapai 10 detik. Jauh berbeda dengan ZigBee yang hanya mencapai 30 milidetik. Hal ini semakin membedakan fungsi dari keduanya. Jika ZigBee lebih difokuskan untuk kebutuhan kontrol yang membutuhkan kecepatan lebih baik, maka bluetooth lebih difokuskan pada besarnya data pada *Personal Area Network*.



Topologi ZigBee.

Tabel Perbandingan ZigBee dengan yang Lainnya.

NAMA PASAR	ZIGBEE	***	WI-FI	BLUETOOTH
Standar	802.15.4	GSM/GPRS/ CDMA 1xRTT	802.11b	802.15.1
Aplikasi	Monitoring & Control	Wide Area Voice & Data	Web, E-mail, Video	Pengganti Kabel
System Resources	4 KB-32 KB	16 MB+	1 MB+	250 KB+
Baterai (hari)	100-1000+	1 s/d 7	0.5 s/d 5	1 s/d 7
Jumlah Node	264	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11000+	720
Jarak (meter)	1-100+	1-1000+	1-100+	1-10+
Keunggulan	Biaya, Tenaga, Keandalan	Jarak dan Kualitas	Fleksibilitas & Kecepatan	Biaya & Menyakinkan

Daya Listrik

Dari segi konsumsi daya juga sangat berbeda. ZigBee yang lebih ditujukan untuk kontrol ini menggunakan daya listrik yang sangat kecil. Di samping itu, kemampuan diam yang dimiliki oleh perangkat ZigBee juga menambah penghematan daya listriknya.

Berbeda dengan bluetooth, yang dalam pengoperasiannya membutuhkan daya yang besar apalagi pada perangkat bluetooth tidak dikenal status diam. Oleh sebab itu jika ZigBee dapat dioperasikan dengan baterai AA atau AAA biasa, bluetooth harus dengan baterai *rechargeable* (contohnya ponsel atau PDA).

ZigBee, Bisnis dan Personal

Perbedaan antara ZigBee dengan bluetooth telah menjadikannya berbeda sasaran pasar. Kecepatan, besar data yang kecil, serta jumlah node yang sangat banyak membuat ZigBee lebih ditujukan untuk sistem kontrol. Tidak hanya kantor dan pabrik saja, tetapi tempat lain seperti tempat tinggal dan pertokoan juga dapat membutuhkan sistem kontrol.

Saat ini kebutuhan kontrol sudah semakin luas. Jika sebagian besar masyarakat khususnya di Indonesia masih menggunakan remote control untuk perangkat-perangkat elektronik tertentu saja seperti TV, Audio-Video, dan AC saja, padahal masih banyak hal lain yang dapat di kontrol. Baik perangkat yang menggunakan sensor maupun yang tidak menggunakan sensor.

Contoh saja untuk lampu. Bila sebuah rumah yang memiliki setidaknya 10 ruangan, maka itu tandanya rumah tersebut dapat memiliki 10 lebih lampu dalam rumah. Hal ini tentu akan merepotkan bila ingin mematikannya, sebab orang tersebut harus masuk dari satu ruangan ke ruangan lain untuk mematikan lampu-lampu tersebut. Namun dengan sebuah alat kontrol lampu khusus, seseorang hanya perlu pergi ke salah stau tempat saja, dan mematikan seluruh lampu dari sana.

Tidak hanya itu, alat kontrol ini dapat dikembangkan untuk tidak hanya mampu untuk mengatur cahaya lampu, melainkan juga dapat digunakan sebagai alat untuk mematikan/mengaktifkan perangkat lain yang menggunakan listrik. Contohnya kunci ataupun alarm rumah.

Hampir semua peralatan dalam pabrik, kantor, toko, ataupun rumah tangga yang terhubung pada listrik membutuhkan alat kontrol. Untuk rumah berukuran kecil mungkin saja tidak terlalu banyak. Namun untuk rumah yang berukuran besar atau hotel tentu akan lebih banyak.

Sedangkan untuk perkantoran yang memiliki banyak ruang sudah pasti membutuhkan banyak sekali peralatan mulai dari lampu, pintu, alarm, AC dan berbagai peralatan tambahan alat kontrol yang tepat dan mampu menampung semua perangkat dalam satu kesatuan tentu akan sangat membantu proses pengamanan. Petugas keamaman pasti tidak akan terlalu kerepotan memeriksa satu ruang ke ruang lagi. Apalagi jika terjadi penambahan ruang atau peralatan lainnya, maka kehadiran ZigBee tentu akan sangat membantu.

ZigBee juga akan sangat membantu jalannya proses produksi di pabrik atau kontrol di supermarket yang memiliki banyak peralatan. Sebab jumlah node yang dapat diakses oleh ZigBee sangat banyak bahkan dapat melebihi dari kebutuhan.

Saingan ZigBee

Bluetooth memang bukan saingan ZigBee, tetapi hal ini bukan berarti ZigBee tanpa saingan. Sebab masih ada yang lainnya yang sudah lebih dulu digunakan sebagai perangkat kontrol. Di antaranya ada Z-Wave dan X-10. Keduanya lebih dulu hadir dan digunakan oleh banyak tempat, baik rumah maupun kantor.

Dengan Z wave, perbedaannya terletak pada dua hal yang sangat signifikan yaitu frekuensi dan *data rates*. Jika ZigBee menggunakan multi-channel frekuensi, maka Z wave hanya satu frekuensi yaitu 868,42 MHz untuk wilayah Eropa atau 8,42 MHz untuk wilayah U.S. Dan data rate yang dimiliki oleh Z-Wave hanya 9,6 Kbps. Frekuensi dan data rate yang terbatas ini mengakibatkan Z wave lebih dominan digunakan untuk tempat tinggal saja atau hanya untuk mengontrol perangkat pencahayaan saja pada tempat-tempat komersial.

Lain halnya dengan X-10 yang berbasiskan pada unidirectional PowerLine Carrier, yaitu carrier yang ada pada aliran listrik biasa di rumah. Teknologi X-10 memang kurang fleksibel, sebab X-10 hanya mampu berinteraksi dengan protokol wireless yang terbatas.

Untuk saat ini, kehadiran ZigBee memang belum dikenal secara luas, apalagi di Indonesia. Mengingat produknya memang belum diproduksi. Namun rencananya, akhir tahun ini banyak perusahaan elektronik baik peralatan sensor/monitoring ataupun kontrol akan mulai memproduksi perangkat ZigBee. Dari peralatan seperti sensor suhu untuk AC/Heater, sensor gas, sensor cahaya, dan masih banyak lagi. Sehingga diharapkan awal tahun 2005 akan banyak masyarakat dunia yang mulai memanfaatkannya baik untuk keperluan personal, bisnis, maupun komersial. ■

LEBIH LANJUT

www.zigbee.com
➔Ini adalah situs resmi ZigBee dari ZigBee Alliance.

File sistem dapat berubah pada waktu Anda menginstalasi *hardware* atau *software*. Anda dapat memantau perubahan pada file sistem dengan *Windows File Protection* dan *System File Checker*.

Gunung Sarjono

Mengatur File Sistem

Menyusuri penyebab suatu masalah bukanlah tugas yang mudah. Untungnya, Windows XP dilengkapi dengan sejumlah tool yang akan membantu Anda untuk mendiagnosis dan memperbaiki setiap kesulitan yang muncul pada PC Anda. Jika suatu pesan *error* atau sejumlah *event* membuat Anda berkesimpulan bahwa file sistem rusak, ada sejumlah cara untuk memperbaikinya.

System Restore memungkinkan Anda untuk kembali ke waktu di mana PC Anda bekerja dengan benar. Pilih *checkpoint* yang diinginkan dan sistem Anda akan dikembalikan ke keadaannya pada waktu tersebut. Sayangnya, System Restore membuat perubahan skala besar pada XP yang mungkin lebih dari yang diperlukan.

Windows File Protection

Pada versi sebelum Windows 2000, menginstalasi *software* tambahan pada *operating system* dapat mengganti file sistem yang di-*share* seperti dynamic-link libraries (file .dll) dan file executable (file .exe). Pada waktu sistem file diganti, kinerja sistem tidak dapat diperkirakan, program bekerja tidak konsisten, dan operating system *fail*.

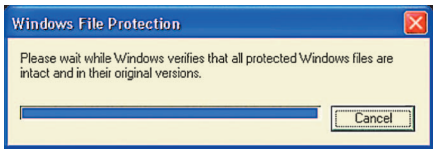
Pada Windows 2000 dan Windows XP, Windows File Protection mencegah penggantian sistem file yang diproteksi seperti file .sys, .dll, .ocx, .ttf, .fon, dan .exe. Windows File Protection berjalan secara *background* dan melindungi semua file yang diinstalasi oleh program Setup Windows.

Windows File Protection mendeteksi, apakah ada program lain yang mencoba mengganti atau memindahkan file sistem yang diproteksi. Windows File Protection mengecek tanda digital file tersebut untuk menentukan apakah file tersebut versi yang benar. Jika tidak, Windows File Protection akan mengganti file dari *back-up* yang disimpan di folder dllcache atau dari CD Windows. Jika Windows File Protection tidak dapat menemukan file yang sesuai, ia meminta Anda memberikan lokasinya.

Secara *default*, Windows File Protection selalu dijalankan dan memungkinkan file Windows yang telah ditandai secara digital menggantikan file yang ada. Biasanya, file yang telah ditandai terdapat pada Windows Service Pack, Hotfix, upgrade operating system, Windows Update, dan Windows Device Manager/Class Installer.

System File Checker

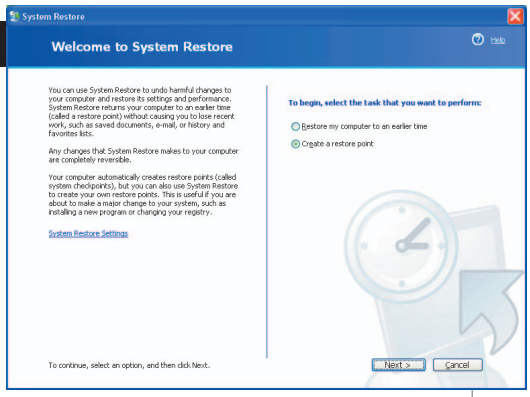
Cara perlindungan kedua yang dilakukan WFP adalah System File Checker(Sfc.exe). Tool ini akan mencari dan memeriksa versi semua file sistem yang diproteksi setelah Anda me-*restart* komputer. Jika sfc menemukan ada file yang diproteksi telah diganti, ia akan mengambil versi file yang benar dari folder dllchache, dan kemudian mengganti file yang tidak benar tersebut. Sfc juga dapat digunakan untuk mengecek dan meng-*update cache* folder jika karena suatu hal rusak atau terkorupsi. Sfc dapat dijalankan dari *Start, Run*. Anda dapat mengontrol kerja tool melalui beragam switch. Untuk memperbaiki cache folder yang rusak, misalnya, klik Start, Run, ketik sfc /scanonce atau sfc /scanboot.



Proses pemeriksaan file sistem oleh *Windows File Protection*.

MEMBUAT SYSTEM RESTORE POINT

- Jika Anda ingin melakukan perubahan ke sistem dengan menginstalasi *software* baru atau memasang *hardware* baru, maka System Restore dapat mengambil gambaran sistem Anda. Anda dapat membuat *restore point* sendiri dan kembali ke *setting* yang lama jika diperlukan. Untuk membuat restore point atau yang dikenal juga dengan 'system checkpoint'.
- Klik *Start*, pilih *All Programs*, pilih *Accessories*, pilih *System Tools*, dan kemudian klik *System Restore*.
- Pilih *Create a restore point* dan kemudian klik *Next*.
- Jika sistem Anda gagal total tekan [F8] pada waktu startup dan pilih *The Last Good Configuration*; setelah masuk ke Windows, jalankan System Restore, pilih *'Restore my computer to an earlier time'* dan pilih restore point Anda.



System Restore.

Pemeriksaan dikontrol oleh nilai registry (SfcScan) pada key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Mengontrol Cache

Cache folder file sistem mempunyai ukuran default 400 MB, yang cukup untuk menyimpan salinan semua sistem file yang dibutuhkan. Namun, jika ruang harddisk tidak mencukupi Anda dapat mengubah ukurannya dengan mengedit key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Klik ganda SfcQuota untuk mengubah nilainya. Default-nya adalah 0xFFFFFFFF yang sama dengan sekitar 400 MB.

Setting default sudah mencukupi untuk semua file sistem, tetapi kadang-kadang cache folder tidak berisi salinan semua file yang dibutuhkan, terlepas dari setting SfcQuota, Windows File Protection akan berhenti memasukkan file ke dllcache jika ruang harddisk yang tersedia kurang dari 600 MB plus ukuran maksimum paging file (yang berarti sama dengan 1-2 GB). Situasi lainnya di mana file tidak akan dimasukkan ke cache folder adalah pada waktu XP diinstalasi melalui jaringan. Perlu dicatat bahwa meskipun semua driver dalam file Driver.cab diproteksi, secara default mereka tidak dimasukkan ke folder dllcache. Untuk memasukkan mereka, jalankan saja sfc dengan switch /scannnow.

Lokasi folder dllcache bergantung kepada nilai SFCDllCacheDir. Nilai default untuk SFCDllCacheDir adalah %SystemRoot%\System32. Nilai SFCDllCacheDir bisa berupa path lokal. Secara default, SFCDllCacheDir tidak ditampilkan pada key HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\Winlogon. Untuk mengubah lokasi cache, Anda harus membuatnya (berupa Expandable String Value).

Tune-up Registry WFP

Pada waktu XP dijalankan, WFP menyinkronisasi (*copy*) setting dari key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Windows File Protection ke key registry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Jika terdapat nilai SfcScan, SfcQuota, atau SFCDllCacheDir pada key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Windows File Protection, mereka akan menggantikan nilai yang sama pada key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Oleh karena itu, Anda harus mengubah nilai key Windows File Protection sebelum merestart komputer supaya setting Anda tidak digantikan pada waktu berikutnya menjalankan Windows.

Mendapatkan Tool Sistem yang Lain

Masukkan CD instalasi XP dan klik *Exit* jika muncul layar tampilan. Buka *My Computer* dan kemudian klik kanan drive CD Anda dan pilih Explore. Cari folder Supports\Tools dan klik ganda Setup.exe. Pada *Windows Support Wizard*, klik *Next*, terima perjanjian lisensi dan kemudian masukkan nama dan organisasi Anda (jika ada). Disarankan untuk memilih *Complete Installation* supaya mendapatkan semua tool. Setelah instalasi selesai, tool pendukung dapat ditemukan di direktori *Program Files\Support Tools*, dengan *shortcut* ke *command prompt*, *file Support Tools Help* dan *Release Notes* pada menu *Start, All Programs*. ■

SETTING NILAI SFCSCAN

0x0 = Jangan scan setelah restart (Setting default).
0x1 = Scan setiap kali di-restart (digunakan jika sfc /scanboot dijalankan).
0x2 = Scan setelah restart berikut (digunakan jika sfc /scanonce dijalankan).

LEBIH LANJUT

http://support.microsoft.com/default.aspx?scid=kb;en-us;222473
➔ *Setting registry* untuk Windows File Protection.

http://support.microsoft.com/default.aspx?scid=kb;en-us;310747
➔ Deskripsi tentang System File Checker Windows XP dan Windows 2003 Server.

http://msdn.microsoft.com/library/en-us/wfp/setup/windows_file_protection_start_page.asp
➔ Referensi mengenai fitur Windows File Protection.

http://msdn.microsoft.com/library/en-us/msi/setup/windows_file_protection_on_windows_2000_and_windows_xp.asp
➔ Informasi tambahan mengenai Windows Installer dan Windows File Protection.

Kami akan menunjukkan bagaimana mengedit *Registry* dan menjaga integritas sistem Anda.

Gunung Sarjono

Password dan Sekuriti

Salah satu aspek Windows di mana pengubahan *Registry* dapat mendatangkan manfaat berdampak luas adalah sekuriti. Selagi *firewall* dan *software* antivirus akan membantu melindungi PC Anda dari ancaman yang berasal dari Internet, perubahan yang Anda buat ke Registry akan membantu menjaga integritas sistem yang di-*share* dengan user lain. Melarang akses ke bagian tertentu dari Windows memungkinkan Anda untuk menghentikan pengrusakan file dan setting yang vital. User yang penasaran dan tidak mempunyai pengetahuan dapat membahayakan Windows Anda. Oleh karena itu, tiba waktunya bagi Anda untuk mengambil kontrol dan mencegah mereka supaya tidak merusakkan PC Anda.

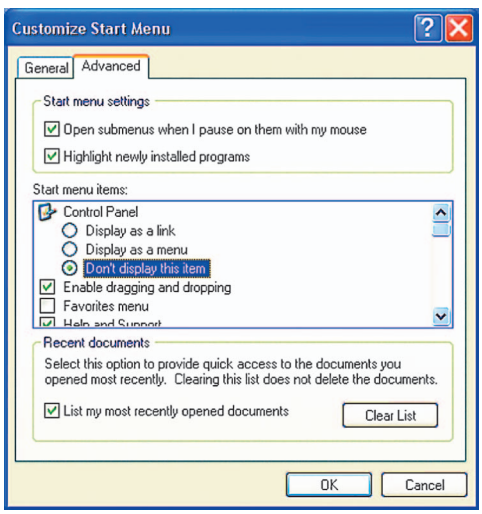
Menyembunyikan Control Panel

Untuk mengakses bermacam-macam *setting* dapat dilakukan dari dalam *Control Panel*. Banyak di antaranya mempunyai dampak yang besar terhadap fungsi sistem dan oleh karena itu mereka harus diubah. Untungnya, jika menggunakan Windows XP, Anda dapat dengan mudah menghilangkan icon Control Panel dan mencegah akses ke semua yang tool yang terdapat di dalamnya dari *Taskbar and Start Menu Properties*. Atau buka Registry Editor dan cari key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer. Buat DWORD Value bernama NoControlPanel dan beri nilai 1 untuk meng-*enable* larangan.

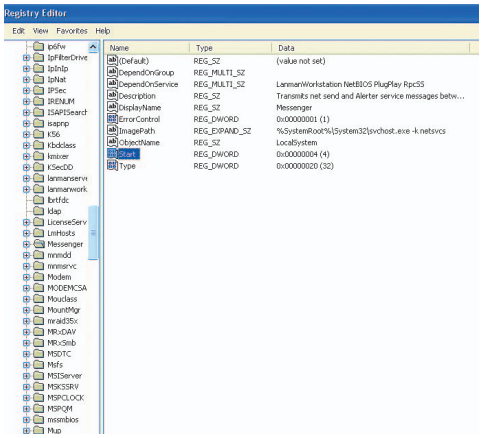
Menyembunyikan Sebagian Applet

Perubahan tersebut tidak hanya akan menghilangkan *Control Panel* dari pandangan, tetapi juga akan menghentikan dijalankannya *shortcut* item Control Panel. Sebagai contoh, klik *Start*, *Run*, dan ketik sysdm.cpl. Biasanya Anda akan dapat menjalankan *System Properties*, tetapi setelah mengubah Registry dan me-restart PC user akan mendapat pesan *'This operation has been cancelled due to restriction in effect on this computer' pada waktu mereka mencoba menjalankan item Control Panel. Please contact your system Administrator.'* Jika mau, Anda dapat mencabut larangan tersebut dengan menghapus entri registry yang baru saja dibuat atau memberinya nilai nol.

Anda lihat bahwa larangan ke Control Panel meliputi semuanya atau tidak sama sekali. Sebagai gantinya mungkin akan lebih masuk akal dengan mengatur akses supaya hanya icon Control Panel tertentu saja yang dapat diakses. Masing-masing applet mempunyai file .cpl-nya sendiri pada folder WINDOWS\System32 yang di-*load* pada waktu



Menghilangkan *Control Panel* dari *Taskbar and Start Menu Properties*.



Mematikan *Messenger* dari *Registry*.

Control Panel dibuka. Dengan mengedit Registry, Anda dapat menentukan applet mana yang tidak ingin di-load. Untuk melarang akses ke suatu item buka Registry Editor dan cari key HKEY_CURRENT_USER\ControlPanel\don't load. Buat String Value, dan beri nama sesuai dengan applet-nya, sebagai contoh sysdm.cpl dan kemudian beri nilai *No* untuk menyembunyikannya atau *Yes* untuk menampilkannya.

Menentukan Model Tampilan Control Panel

Tampilan default Control Panel pada Windows XP membagi applet ke dalam kategori-kategori. Perubahan Registry ini memaksa digunakannya model baru atau klasik. Pada Registry Editor cari key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Buat DWORD Value bernama ForceClassicControlPanel dan beri nilai 1 untuk memastikan model klasik ditampilkan atau 0 untuk model baru.

Kontrol User

Dengan adanya berbagai aplikasi yang terintalasi pada PC Anda, ada batas di mana Anda tidak ingin user mempunyai akses. Dengan mengedit Registry, Anda dapat memisahkan program-program yang tidak boleh mereka gunakan. Buka Registry Editor dan cari key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun. Dari situ Anda dapat menentukan aplikasi mana yang tidak boleh diakses oleh user. Buat *String Value* untuk setiap aplikasi dengan menggunakan nomor urut sebagai namanya, misalnya 1, 2, 3, 4, dan seterusnya. Nilai untuk masing-masing harus file executable .exe yang menjalankan program.

Pada Windows XP, proses untuk melarang akses ke aplikasi sedikit berbeda. Cari key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer dan buat DWORD Value bernama DisallowRun dan set nilainya ke 1 untuk meng-enable larangan aplikasi. Kemudian buat key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun dan dengan cara yang sama seperti sebelumnya, masukkan program yang tidak boleh dijalankan oleh user ke dalam key tersebut.

Sekuriti Sistem

Dengan adanya beberapa orang yang dapat mengakses komputer Anda, sangat penting untuk mengatur sekuriti seketat mungkin. Windows XP dapat menyimpan informasi otentikasi dan password .Net pada harddisk Anda. Jika Anda yakin ada orang lain yang mungkin mencoba menggunakan informasi tersebut, edit registry supaya informasi tersebut tidak lagi disimpan pada masa yang akan datang. Pertama cari key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa. Kemudian edit atau buat DWORD Value bernama disabeldomaincreds dan beri nilai 1 untuk mematikan penyimpanan. Hapus nilai atau ganti ke 0 untuk menyalakan kembali penyimpanan.

Jika Anda mengalami masalah dengan Windows XP, maka tool *System Restore* dapat mengembalikan sesuatunya seperti semula. Namun, jika Anda pemerhati sekuriti, maka Anda mungkin akan menjauhkan fitur ini dari jangkauan user karena ia juga mengubah registry pada waktu dijalankan. Untuk mematikan System Restore pada menu Start, cari key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore. Ubah nilai DWORD Value bernama DisableSR menjadi 1. Kemungkinan lain, Anda dapat melarang akses dengan membuat DWORD Value bernama DisableConfig dan beri nilai 1.

Melarang Akses ke Setting Interface Tertentu

Dari menu *Start*, Anda bisa mengakses ke submenu yang lain. Untuk mematikan akses ke submenu, cari key HKEY_CLASSES_ROOT\CLSID\{5b4dae26-b807-11d0-9815-00c04fd91972}. Ganti nama key dengan menambahkan tanda "-" di depan {5b4dae26-b807-11d0-9815-00c04fd91972}.

Anda dapat mencegah penambahan toolbar ke Taskbar dari key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer. Buat DWORD Value bernama NoToolbarOnTaskbar dengan nilai 1.

Menghapus perintah Run dari menu Start mencegah user menjalankan semua jenis aplikasi. Buka key HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\policies\Explorer. Buat DWORD Value bernama NoRun dan beri nilai 1.

Menjaga Informasi Pribadi Tetap Aman

File paging dapat menyimpan informasi pribadi. Untuk membersihkan isinya pada waktu mematikan komputer, buka key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management, lalu buat DWORD Value bernama ClearPageFileAtShutdown dengan nilai 1.

Bersihkan semua file temporer dari dalam IE pada waktu browser ditutup. Buka key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache, dan kemudian buat DWORD Value bernama Persistent dan beri nilai 0.

Layanan *Messenger* kadang-kadang digunakan untuk mengirim *spam* melalui Internet. Buka key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger, dan kemudian ubah nilai Start ke 4 supaya layanan tersebut dimatikan. ■

LEBIH LANJUT

support.microsoft.com/?kbid=313808
➔Ini merupakan alamat situs web untuk mendapatkan daftar lengkap mengenai file *Control Panel*.

Windows XP dapat—dan akan—menjalankan sejumlah bagian yang tidak diinginkan pada waktu *startup*. Kita akan melihat bagaimana mencegahnya.

Gunung Sarjono

Startup dengan Lancar

▶Windows XP mungkin tampak sebagai satu unit yang terpadu, tetapi kenyataan yang didapat sedikit berbeda. *Operating system* yang sebenarnya dibangun dari ratusan modul komponen terpisah di atas kernel itu sendiri, dan banyak di-antaranya secara opsional atau kadang-kadang dipaksa untuk dijalankan sebagai bagian dari prosedur *boot* Window.

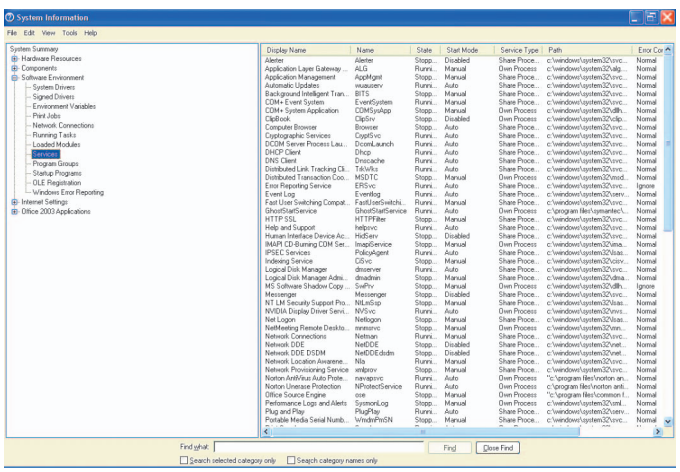
Seperti semua operating system modern, Windows XP dapat menjalankan kode lain pada waktu boot untuk melengkapi OS itu sendiri, atau melakukan tugas tertentu. Bersama Windows XP, potongan kode ini dapat berupa program *execubtable* (yang bisa Anda jalankan dari Desktop) dan Windows Service.

Microsoft menyebut *Service* sebagai suatu program, rutin atau proses yang melakukan fungsi tertentu untuk mendukung program lain. Dengan kata lain, Service adalah bagian terpisah dari kode yang didesain untuk melakukan suatu fungsi, baik untuk Windows itu sendiri atau aplikasi yang diinstalasi pada PC Anda.

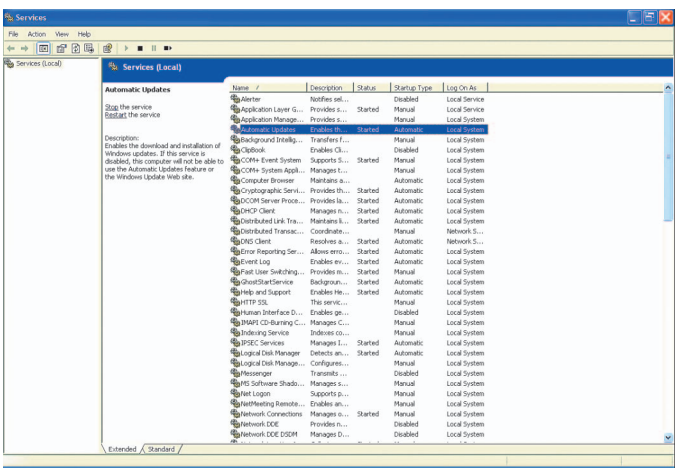
Sebagai contoh, suatu *hardware* mungkin membutuhkan Service supaya dapat bekerja dengan benar, sementara Windows itu sendiri bergantung kepada banyak service untuk bekerja, termasuk yang menangani tool perekaman CD *built-in*, pengambilan gambar dari scanner dan kamera, serta banyak lagi.

Menjalankan Service

Service umumnya dijalankan pada akhir *booting* sesaat sebelum Anda tiba di Desktop. Banyak service standar yang



Daftar *service* pada *System Information*.



Mengontrol *service* dari *snap-in Services*.

dibutuhkan sebelum XP dapat mengambil input dari Anda melalui mouse atau keyboard, dan layar Logon itu sendiri sangat bergantung kepada beberapa service, terutama jika Anda menjalankan *Fast User Switching*.

Service dapat dihentikan atau dijalankan setiap waktu, baik oleh sistem maupun Anda sendiri, meskipun menghentikan service yang sangat penting bagi sistem merupakan tindakan yang nekad. Pada sistem Windows XP Home, banyak service yang dijalankan sebelum Anda melihat *desktop*, beberapa diantaranya tidak akan Anda butuhkan, dan masing-masing memakan memory.

Sebelum menghentikan service yang tidak dibutuhkan atau inginkan, Anda perlu melihat apa yang sedang berjalan. System Information berguna dalam situasi ini—buka kotak dialog Run Start Menu, kemudian ketik msinfo32 dan klik OK. Pada panel sebelah kiri, perluas *tree Software Environtment* kemudian klik *Services*. Setelah beberapa detik, Anda akan melihat daftar service yang saat itu tersedia pada sistem Anda, dan apakah mereka sedang berjalan atau tidak. Tampilan ini hanya bersifat informatis dan Anda tidak bisa melakukan apa-apa terhadap daftar tersebut, tetapi kita nanti akan menggunakan lagi program *System Information*, jadi biarkan saja tetap terbuka.

Management Console

Untuk mengontrol service mana yang dijalankan Windows XP pada waktu *startup*, Anda harus menjalankan *snap-in Services* pada *Microsoft Management Console*. Bergantung kepada vendor PC Anda, ini mungkin saja ditampilkan atau tidak ditampilan pada *Start Menu*. Jika tidak, Anda bisa menjalankannya sendiri—untuk informasi lebih lengkap lihat kotak "Mendapatkan Kontrol atas Tool Administrasi Sistem." Jika Anda mempunyai Management Console pada Start Menu, jalankan dan pilih tab *Services*. Cara cepat untuk mengatur service tanpa perlu menjalankan Microsoft Management Console adalah dengan menjalankan kotak dialog Run Start Menu, ketik services.msc, dan kemudian klik OK.

Sebelum Anda melakukan sesuatu, lihat di bawah jendela yang baru saja dibuka dan Anda akan melihat dua tab bernama *Extended* dan *Standard*. Pastikan Anda berada dalam mode Extended—tidak lebih kompleks, tetapi menyediakan informasi lebih banyak.

Pilih suatu service dan Anda akan melihat beberapa keterangan yang memberitahu Anda lebih banyak tentang service tersebut. Pada jendela utama, Anda juga akan melihat bahwa masing-masing service mempunyai kolom, yang menampilkan apakah service sedang berjalan, dan bagaimana ia dijalankan.

Sekarang, Anda bisa mencegah supaya service tidak dijalankan pada waktu startup, dan tidak sulit untuk melakukannya. Cari service yang ingin Anda hentikan, dan kemudian klik ganda service tersebut. Pada tab General, Anda akan melihat setting bernama *Startup type*. Biasanya ini diset ke *Automatic*, yang berarti service dijalankan pada waktu startup setiap kali Anda booting. Ganti ke *Manual*. Ini berarti Anda bisa menjalankan sendiri service tersebut, tetapi yang lebih penting, setiap bagian Windows yang bergantung kepadanya dapat menjalankannya pada waktu benar-benar dibutuhkan.

Hentikan service yang tidak Anda inginan dengan mengklik tombol Stop. Jangan gunakan *Disabled*, kecuali jika Anda benar-benar tahu apa yang Anda lakukan, karena menghentikan service yang salah bisa menyebabkan gagalnya booting.

Program Auto-run

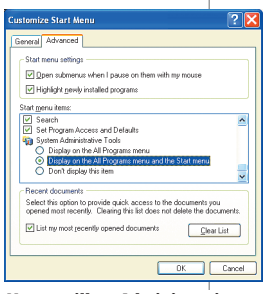
Tentu saja, Windows XP juga menjalankan program pada waktu *startup* sama seperti versi lama dari *operating system* tersebut. Ini bisa dari aplikasi pembantu untuk hardware dan *system tray* atau *Notification Area* sampai aplikasi berbeban berat. Anda tidak selalu menginginkan program tersebut, dan mematikan mereka tidak selalu menjadi jalan terbaik. Di bawah Windows versi lama, program bisa dijalankan secara otomatis bersama Windows dengan memasukkannya ke folder Startup atau dengan menambahkan suatu key ke bagian tertentu dari Registry.

Pada Windows XP, hal ini sedikit lebih rumit karena setiap user dapat mempunyai folder Startup terpisah di samping yang global atau umum. Untuk mengetahui apa yang dijalankan pada waktu Anda mem-boot Windows, lihat lagi program *System Information* dan pindahklah ke *Startup Programs* di dalam hirarki *Software Environment*. Di situ Anda akan meihat daftar lengkap aplikasi global dan aplikasi yang dijalankan per-*user*. ■

MENDAPATKAN KONTROL ATAS TOOL ADMINISTRASI SISTEM

■ Jika merakit atau menginstalasi sendiri Windows XP pada sistem yang sudah terinstalasi dengan Windows versi lama, maka Anda akan mempunyai kontrol penuh terhadap lokasi penginstalasan Windows dan bagaimana konfigurasi mereka. Di lain pihak, jika Anda membeli sistem yang sudah dilengkapi dengan Windows XP, maka pada bagian tertentu Anda mungkin harus meminta vendor PC Anda untuk mengesetnya.

Salah satu contoh adalah apakah Microsoft Management Console tersedia untuk Anda atau tidak. Pada banyak sistem yang didesain untuk penggunaan keluarga, MMC tidak ada pada *Start Menu*. Yang mengganggu adalah program tersebut masih ada di situ, jika Anda tahu di mana menemukannya.



Menampilkan Administrative Tools dari Taskbar and Start Menu Properties.

Untungnya, mengembalikan MMC ke Start Menu tidak begitu sulit jika Anda tahu apa yang Anda lakukan. Pertama, Anda harus masuk dengan hak Administrator. Klik kanan *Taskbar*, pilih *Properties*, dan kemudian klik tab *Start Menu*. Klik *Customize*, dan kemudian klik tab *Advanced*. Geser daftar Start Menu item ke bawah, dan kemudian jalankan *System Administrative Tools*.

LEBIH LANJUT

http://support.microsoft.com/default.aspx?scid=kb;en-us;314488

➔ Menjelaskan bagaimana cara mengubah daftar program yang dijalankan pada waktu Anda menjalankan Windows XP.