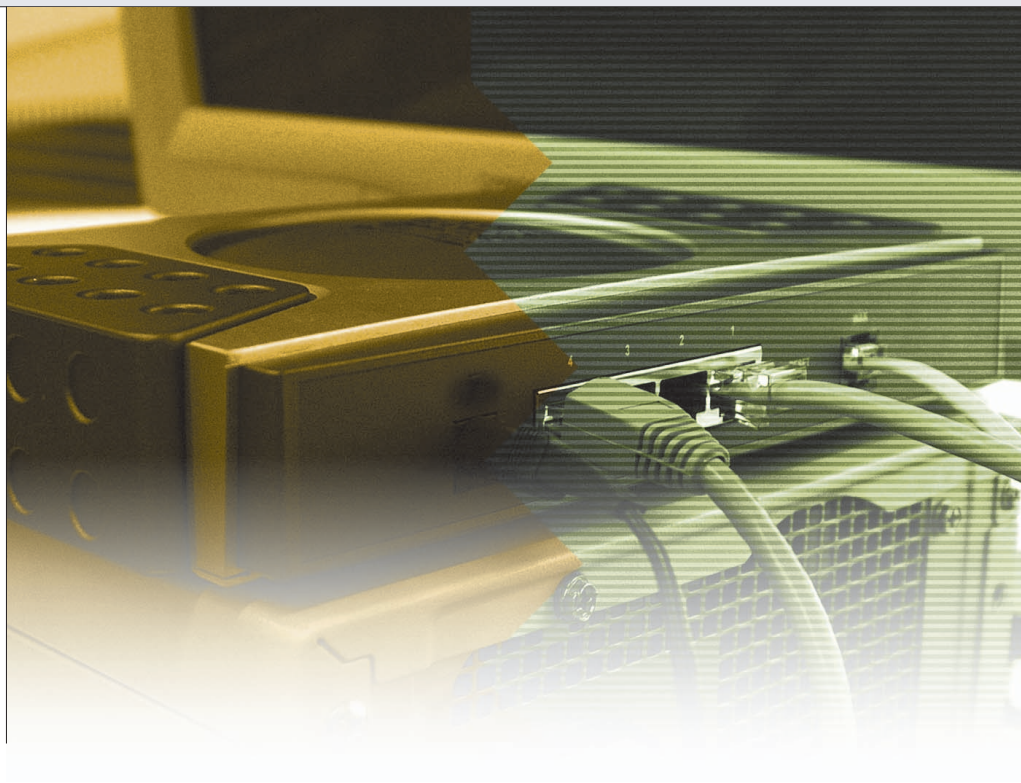


Kekuatan dari OSPF ada pada sistem hirarkinya yang diterapkan dalam sistem area. Penyebaran informasi *routing* menjadi lebih teratur dan juga mudah untuk di-*troubleshooting*.

Hayri

Bagian 2 dari 2 Artikel

OSPF, Routing Protokol untuk Jaringan Lokal

Pada edisi sebelumnya, telah dibahas bagaimana sebuah router OSPF memulai aktivitasnya dalam melakukan pertukaran informasi *routing* dengan sesamanya. Langkah pertama yang harus dilakukan oleh OSPF adalah membentuk komunikasi dengan para router tetangganya. Tujuannya adalah agar informasi apa yang belum diketahui oleh router tersebut dapat diberi tahu oleh router tetangganya.

Begitu pula router tetangga tersebut juga akan menerima informasi dari router lain yang bertindak sebagai tetangganya. Sehingga pada akhirnya seluruh informasi yang ada dalam sebuah jaringan dapat diketahui oleh semua router yang ada dalam jaringan tersebut. Kejadian ini sering disebut dengan istilah *Convergence*.

Setelah router membentuk komunikasi dengan para tetangganya, maka proses pertukaran informasi routing berlangsung dengan menggunakan bantuan beberapa paket khusus yang bertugas membawa informasi routing tersebut. Paket-paket tersebut sering disebut dengan istilah *Link State Advertisement packet* (LSA packet). Selain dari hello packet, routing protokol OSPF juga sangat bergantung kepada paket jenis ini untuk dapat bekerja.

OSPF memang memiliki sistem *update* informasi routing yang cukup teratur dengan rapi. Teknologinya menentukan jalur terpendek dengan algoritma *Shortest Path First* (SPF) juga sangat hebat. Meskipun terbentang banyak jalan menuju ke sebuah lokasi, namun OSPF dapat menentukan jalan mana yang paling baik dengan sangat tepat. Sehingga komunikasi data Anda menjadi lancar dan efisien.

Namun ada satu lagi keunggulan OSPF, yaitu konsep jaringan hirarki yang membuat proses update informasinya lebih termanajemen dengan baik. Dalam menerapkan konsep hirarki ini, OSPF menggunakan pembagian jaringan berdasarkan konsep area-area. Pembagian berdasarkan area ini yang juga merupakan salah satu kelebihan OSPF.

Untuk Apa Konsep Area dalam OSPF?

OSPF dibuat dan dirancang untuk melayani jaringan lokal berskala besar. Artinya OSPF haruslah memiliki nilai skalabilitas yang tinggi, tidak mudah habis atau "mentok" karena jaringan yang semakin diperbesar. Namun nyatanya pada penerapan OSPF biasa, beberapa kejadian juga dapat membuat router OSPF kewalahan dalam menangani jaringan yang semakin membesar. Router OSPF akan mencapai titik kewalahan ketika:

- Semakin membesarnya area jaringan yang dilayaninya akan semakin banyak informasi yang saling dipertukarkan. Semakin banyak router yang perlu dilayani untuk menjadi *neighbour* dan *adjacence*. Dan semakin banyak pula proses pertukaran informasi routing terjadi. Hal ini akan membuat router OSPF membutuhkan

lebih banyak sumber memory dan processor. Jika router tersebut tidak dilengkapi dengan memory dan processor yang tinggi, maka masalah akan terjadi pada router ini.

- Topology table akan semakin membesar dengan semakin besarnya jaringan. Topology table memang harus ada dalam OSPF karena OSPF termasuk routing protocol jenis Link State. Topology table menrupakan tabel kumpulan informasi state seluruh link yang ada dalam jaringan tersebut. Dengan semakin membesarnya jaringan, maka topology table juga semakin membengkak besarnya. Pembengkakan ini akan mengakibatkan router menjadi lama dalam menentukan sebuah jalur terbaik yang akan dimasukkan ke routing table. Dengan demikian, performa *forwarding* data juga menjadi lamban.
- Topology table yang semakin membesar akan mengakibatkan routing table semakin membesar pula. Routing table merupakan kumpulan informasi rute menuju ke suatu lokasi tertentu. Namun, rute-rute yang ada di dalamnya sudah merupakan rute terbaik yang dipilih menggunakan algoritma Djikstra. Routing table yang panjang dan besar akan mengakibatkan pencarian sebuah jalan ketika ingin digunakan menjadi lambat, sehingga proses forwarding data juga semakin lambat dan menguras tenaga processor dan memory. Performa router menjadi berkurang.

Melihat titik-titik kelemahan OSPF dalam melayani jaringan yang berkembang pesat, maka para pencipta routing protokol ini juga tidak membiarkannya saja. Untuk itu, routing protokol ini dilengkapi dengan sistem hirarki yang berupa pengelompokan router-router OSPF dalam area. Dengan membagi-bagi router dalam jaringan menjadi tersegmen, maka akan banyak keuntungan yang akan didapat, khususnya untuk menangani masalah ketika jaringan semakin membesar dan perangkatnya semakin kehabisan tenaga. Untuk tujuan inilah konsep area diciptakan dalam routing protokol OSPF.

Bagaimana Konsep Area Dapat Mengurangi Masalah?

Ketika sebuah jaringan semakin membesar dan membesar terus, routing protokol OSPF tidak efektif lagi jika dijalankan dengan hanya menggunakan satu area saja. Seperti telah Anda ketahui, OSPF merupakan routing protokol berjenis Link State. Maksudnya, routing protokol ini akan mengumpulkan data dari status-status setiap link yang ada dalam jaringan OSPF tersebut.

Apa jadinya jika jaringan OSPF tersebut terdiri dari ratusan bahkan ribuan link di dalamnya? Tentu proses pengumpulannya saja akan memakan waktu lama dan resource processor yang banyak. Setelah itu, proses penentuan jalur terbaik yang dilakukan OSPF juga menjadi sangat lambat.

Berdasarkan limitasi inilah konsep area dibuat dalam OSPF. Tujuannya adalah untuk mengurangi jumlah link-link yang dipantau dan dimonitor statusnya agar penyebaran informasinya menjadi cepat dan efisien serta tidak menjadi rakus akan tenaga processing dari perangkat router yang menjalankannya.

Bagaimana Informasi Link State Disebarkan?

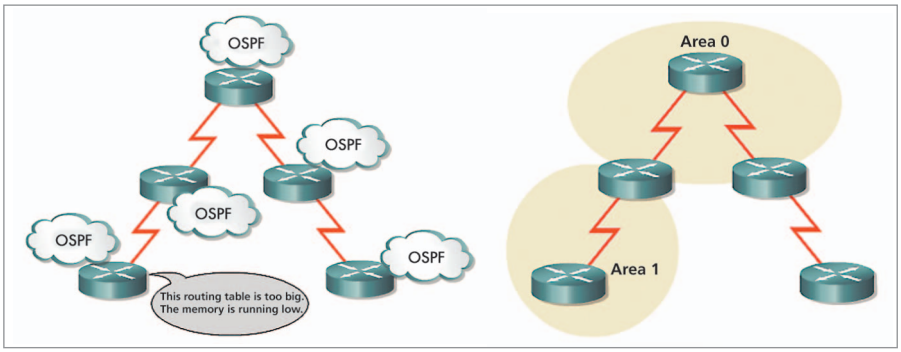
Untuk menyebarkan informasi Link State ke seluruh router dalam jaringan, OSPF memiliki sebuah sistem khusus untuk itu. Sistem ini sering disebut dengan istilah *Link State Advertisement* (LSA). Dalam menyebarkan informasi ini, sistem LSA menggunakan paket-paket khusus yang membawa informasi berupa status-status link yang ada dalam sebuah router. Paket ini kemudian dapat tersebar ke seluruh jaringan OSPF. Semua informasi link yang ada dalam router dikumpulkan oleh proses OSPF, kemudian dibungkus dengan paket LSA ini dan kemudian dikirimkan ke seluruh jaringan OSPF.

Apa sih Paket LSA?

Seperti telah dijelaskan di atas, paket LSA di dalamnya akan berisi informasi seputar link-link yang ada dalam sebuah router dan statusnya masing-masing. Paket LSA ini kemudian disebarkan ke router-router lain yang menjadi neighbour dari router tersebut. Setelah informasi sampai ke router lain, maka router tersebut juga akan menyebarkan LSA miliknya ke router pengirim dan ke router lain.

Pertukaran paket LSA ini tidak terjadi hanya pada saat awal terbentuknya sebuah jaringan OSPF, melainkan terus-menerus jika ada perubahan link status dalam sebuah jaringan OSPF. Namun, LSA yang disebarkan kali pertama tentu berbeda dengan yang disebarkan berikutnya. Karena LSA yang pertama merupakan informasi yang terlengkap seputar status dari link-link dalam jaringan, sedangkan LSA berikutnya hanyalah merupakan *update* dari perubahan status yang terjadi.

Paket-paket LSA juga dibagi menjadi beberapa jenis. Pembagian ini dibuat berdasarkan informasi yang terkandung di dalamnya dan untuk siapa LSA ini ditujukan. Untuk membedakan jenis-jenisnya ini, OSPF membagi paket LSA nya menjadi tujuh tipe. Masing-masing tipe memiliki kegunaannya masing-masing dalam membawa informasi Link State. Anda dapat melihat kegunaan masing-masing paket pada tabel "Tipe-tipe LSA packet".



Semakin membengkaknya jaringan lokal, akan membuat router-router OSPF menjadi bekerja berat. Konsep area akan menuntaskan masalah ini.

Tipe-tipe Router OSPF

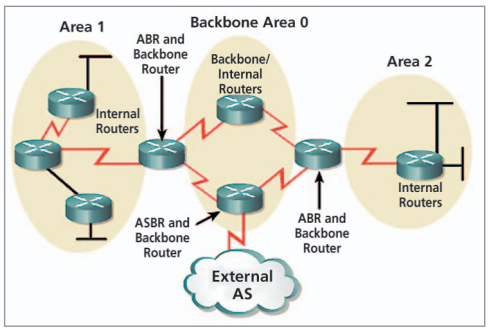
Seperti telah Anda ketahui, OSPF menggunakan konsep area dalam menjamin agar penyebaran informasi tetap teratur baik. Dengan adanya sistem area-area ini, OSPF membedakan lagi tipe-tipe router yang berada di dalam jaringannya. Tipe-tipe router ini dikategorikan berdasarkan letak dan perannya dalam jaringan OSPF yang terdiri dari lebih dari satu area. Di mana letak sebuah router dalam jaringan OSPF juga sangat berpengaruh terhadap fungsinya. Jadi dengan demikian, selain menunjukkan lokasi di mana router tersebut berada, nama-nama tipe router ini juga akan menunjukkan fungsinya. Berikut ini adalah beberapa tipe router OSPF berdasarkan letaknya dan juga sekaligus fungsinya:

- **Internal Router**

Router yang digolongkan sebagai internal router adalah router-router yang berada dalam satu area yang sama. Router-router dalam area yang sama akan menanggap router lain yang ada dalam area tersebut adalah internal router. Internal router tidak memiliki koneksi-koneksi dengan area lain, sehingga fungsinya hanya memberikan dan menerima informasi dari dan ke dalam area tersebut. Tugas internal router adalah me-*maintain* database topologi dan *routing table* yang akurat untuk setiap subnet yang ada dalam areanya. Router jenis ini melakukan *flooding* LSA informasi yang dimilikinya ini hanya kepada router lain yang dianggapnya sebagai internal router.

- **Backbone Router**

Salah satu peraturan yang diterapkan dalam routing protokol OSPF adalah setiap area yang ada dalam jaringan OSPF harus terkoneksi dengan sebuah area yang dianggap sebagai *backbone area*. Backbone area biasanya ditandai dengan penomoran 0.0.0.0 atau sering disebut dengan istilah Area 0. Router-router yang sepenuhnya berada di dalam Area 0 ini dinamai dengan istilah *backbone router*. Backbone router memiliki semua informasi topologi dan routing yang ada dalam jaringan OSPF tersebut.



Pembagian tipe-tipe router OSPF berdasarkan fungsi dan letaknya dalam jaringan OSPF yang berhirarki.

Tipe-tipe LSA Packet.

TIPE LSA	NAMA	DESKRIPSI
1	Router link entry	Di-generate oleh setiap router OSPF untuk areanya di mana router tersebut berada. LSA tipe ini menginformasikan state-state sebuah router ke seluruh areanya. Link status dan cost merupakan parameter yang dikirimkan oleh paket LSA ini.
2	Network link entry	Tipe LSA ini di-generate oleh router OSPF yang terkoneksi menggunakan media broadcast multiaccess seperti ethernet. LSA tipe ini mendeskripsikan informasi mengenai state dari semua router yang terkoneksi ke dalam jaringan broadcast multiaccess. Biasanya router DR adalah pembuat paket jenis ini.
3	Summary link entry	Router yang berfungsi sebagai ABR yang akan meng-generate paket LSA ini. LSA Tipe 3 akan membawa informasi link-link yang ada di antara ABR dengan router internal yang ada dalam satu area. Jadi informasi dari area lain akan dibawa menuju backbone area menggunakan paket LSA jenis ini.
4	Summary link entry	LSA tipe ini hampir sama dengan LSA tipe 3 hanya bedanya LSA ini merupakan paket informasi yang dikirimkan ke router ASBR.
5	Autonomous system external link entry	LSA tipe 5 di-generate oleh router ASBR. Di dalamnya berisikan informasi state dan rute dari link-link di luar routing protocol OSPF.
6	Multicast OSPF	LSA tipe ini digunakan untuk membuat multicast distribution tree dengan memanfaatkan Link State database yang dikumpulkan oleh OSPF.
7	Autonomous external system entry	Paket LSA jenis ini di-generate oleh router ASBR yang terkoneksi ke NSSA.

- **Area Border Router (ABR)**

Sesuai dengan istilah yang ada di dalam namanya "Border", router yang tergolong dalam jenis ini adalah router yang bertindak sebagai penghubung atau perbatasan. Yang dihubungkan oleh router jenis ini adalah area-area yang ada dalam jaringan OSPF. Namun karena adanya konsep backbone area dalam OSPF, maka tugas ABR hanyalah melakukan penyatuan antara Area 0 dengan area-area lainnya. Jadi di dalam sebuah router ABR terdapat koneksi ke dua area berbeda, satu koneksi ke area 0 dan satu lagi ke area lain.

Router ABR menyimpan dan menjaga informasi setiap area yang terkoneksi dengannya. Tugasnya juga adalah menyebarkan informasi tersebut ke masing-masing areanya. Namun, penyebaran informasi ini dilakukan dengan menggunakan LSA khusus yang isinya adalah *summarization* dari setiap segment IP yang ada dalam jaringan

tersebut. Dengan adanya summary update ini, maka proses pertukaran informasi routing ini tidak terlalu memakan banyak resource processing dari router dan juga tidak memakan banyak bandwidth hanya untuk update ini.

- **Autonomous System Boundary Router (ASBR)**

Sekelompok router yang membentuk jaringan yang masih berada dalam satu hak administrasi, satu kepemilikan, satu kepentingan, dan dikonfigurasi menggunakan policy yang sama, dalam dunia jaringan komunikasi data sering disebut dengan istilah Autonomous System (AS). Biasanya dalam satu AS, router-router di dalamnya dapat bebas berkomunikasi dan memberikan informasi. Umumnya, routing protocol yang digunakan untuk bertukar informasi routing adalah sama pada semua router di dalamnya. Jika menggunakan OSPF, maka semuanya tentu juga menggunakan OSPF.

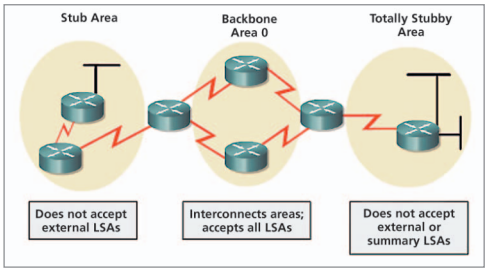
Namun, ada kasus-kasus di mana sebuah segmen jaringan tidak memungkinkan untuk menggunakan OSPF sebagai routing protokolnya. Misalkan kemampuan router yang tidak memadai, atau kekurangan sumber daya manusia yang paham akan OSPF, dan banyak lagi. Oleh sebab itu, untuk segmen ini digunakanlah routing protocol IGP (*Interior Gateway Protocol*) lain seperti misalnya RIP. Karena menggunakan routing protocol lain, maka oleh jaringan OSPF segmen jaringan ini dianggap sebagai AS lain.

Untuk melayani kepentingan ini, OSPF sudah menyiapkan satu tipe router yang memiliki kemampuan ini. OSPF mengategorikan router yang menjalankan dua routing protokol di dalamnya, yaitu OSPF dengan routing protokol IGP lainnya seperti misalnya RIP, IGRP, EIGRP, dan IS-IS, kemudian keduanya dapat saling bertukar informasi routing, disebut sebagai *Autonomous System Border Router* (ASBR).

Router ASBR dapat diletakkan di mana saja dalam jaringan, namun yang pasti router tersebut haruslah menjadi anggota dari Area 0-nya OSPF. Hal ini dikarenakan data yang meninggalkan jaringan OSPF juga dianggap sebagai meninggalkan sebuah area. Karena adanya peraturan OSPF yang mengharuskan setiap area terkoneksi ke backbone area, maka ASBR harus diletakkan di dalam backbone area.

Ada Berapa Jenis Area dalam OSPF?

Setelah membagi-bagi jaringan menjadi bersistem area dan membagi router-router di dalamnya menjadi beberapa jenis berdasarkan posisinya dalam sebuah area, OSPF masih membagi lagi jenis-jenis area yang ada di dalamnya. Jenis-jenis area OSPF ini menunjukkan di mana area tersebut berada dan bagaimana karakteristik area tersebut dalam jaringan. Berikut ini adalah jenis-jenis area dalam OSPF:



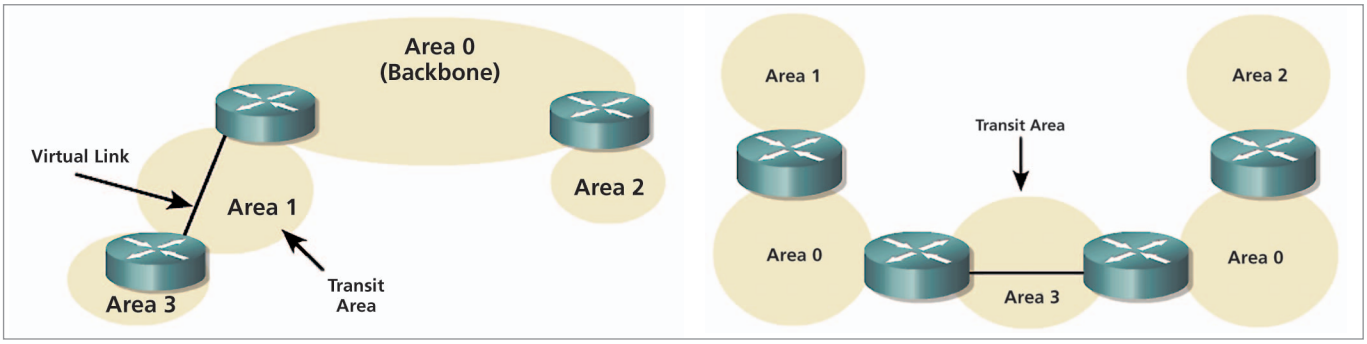
Jenis-jenis area dibagi berdasarkan kemampuannya mengirim dan menerima LSA.

- **Backbone Area**

Backbone area adalah area tempat bertemunya seluruh area-area lain yang ada dalam jaringan OSPF. Area ini sering ditandai dengan angka 0 atau disebut Area 0. Area ini dapat dilewati oleh semua tipe LSA kecuali LSA tipe 7 yang sudah pasti akan ditransfer menjadi LSA tipe 5 oleh ABR.

- **Standar Area**

Area jenis ini merupakan area-area lain selain area 0 dan tanpa disertai dengan konfigurasi apapun. Maksudnya area ini tidak dimodifikasi macam-macam. Semua router yang ada dalam area ini akan mengetahui informasi Link State yang sama karena mereka semua akan saling membentuk *adjacent* dan saling bertukar informasi secara langsung. Dengan demikian, semua router yang ada dalam area ini akan memiliki topology database yang



Konsep *backbone area* memiliki peraturan semua area yang ada harus terkoneksi dengan area 0. Teknologi *Virtual link* memungkinkan peraturan ini tetap dipatuhi meskipun secara fisiknya tidak ada koneksi.

sama, namun routing table-nya mungkin saja berbeda.

● Stub Area

Stub dalam arti harafiahnya adalah ujung atau sisi paling akhir. Istilah ini memang digunakan dalam jaringan OSPF untuk menjuluki sebuah area atau lebih yang letaknya berada paling ujung dan tidak ada cabang-cabangnya lagi. *Stub area* merupakan area tanpa jalan lain lagi untuk dapat menuju ke jaringan dengan segmen lain.

Area jenis ini memiliki karakteristik tidak menerima LSA tipe 4 dan 5. Artinya adalah area jenis ini tidak menerima paket LSA yang berasal dari area lain yang dihantarkan oleh router ABR dan tidak menerima paket LSA yang berasal dari routing protokol lain yang keluar dari router ASBR (LSA tipe 4 dan 5). Jadi dengan kata lain, router ini hanya menerima informasi dari router-router lain yang berada dalam satu area, tidak ada informasi routing baru di router.

Namun, yang menjadi pertanyaan selanjutnya adalah bagaimana area jenis ini dapat berkomunikasi dengan dunia luar kalau tidak ada informasi routing yang dapat diterimanya dari dunia luar. Jawabannya adalah dengan menggunakan *default route* yang akan bertugas menerima dan meneruskan semua informasi yang ingin keluar dari area tersebut. Dengan default route, maka seluruh *traffic* tidak akan dibuang ke mana-mana kecuali ke segmen jaringan di mana IP default route tersebut berada.

● Totally Stub Area

Mendengar namanya saja, mungkin Anda sudah bisa menangkap artinya bahwa area jenis ini adalah stub area yang lebih diperketat lagi perbatasannya. *Totally stub area* tidak akan pernah menerima informasi routing apapun dari jaringan di luar jaringan mereka. Area ini akan memblokir LSA tipe 3, 4, dan 5 sehingga tidak ada informasi yang dapat masuk ke area ini. Area jenis ini juga sama dengan stub area, yaitu mengandalkan default route untuk dapat menjangkau dunia luar.

● Not So Stubby Area (NSSA)

Stub tetapi tidak terlalu stub, itu adalah arti harafiahnya dari area jenis ini. Maksudnya adalah sebuah stub area yang masih memiliki kemampuan spesial, tidak seperti stub area biasa. Kemampuan spesial ini adalah router ini masih tetap mendapatkan informasi routing namun tidak semuanya. Informasi routing yang didapat oleh area jenis ini adalah hanya external route yang diterimanya bukan dari backbone area. Maksudnya adalah router ini masih dapat menerima informasi yang berasal dari segmen jaringan lain di bawahnya yang tidak terkoneksi ke backbone area.

Misalnya Anda memiliki sebuah area yang terdiri dari tiga buah router. Salah satu router terkoneksi dengan backbone area dan koneksinya hanya berjumlah satu buah saja. Area ini sudah dapat disebut sebagai stub area. Namun nyatanya, area ini memiliki satu segmen jaringan lain yang menjalankan routing protokol RIP misalnya. Jika Anda masih mengonfigurasi area ini sebagai Stub area, maka area ini tidak menerima informasi routing yang berasal dari jaringan RIP. Namun konfigurasilah dengan NSSA, maka area ini bisa mengenali segmen jaringan yang dilayani RIP.

Performa Hebat Didukung Perangkat Hebat

Jaringan Anda boleh bertambah besar, berapapun subnet IP di dalamnya, berapapun klien yang harus dilayani, dan berapapun server di belakangnya boleh-boleh saja bertambah. Percayakan saja pada routing protokol OSPF yang mengatur semua penyebaran informasi routing-nya. Namun ada satu yang perlu Anda perhatikan juga, ketika jaringan membesar dan routing protokol OSPF sudah terpecah-pecah menjadi beberapa area, perangkat router Anda juga harus mendukung kebutuhan tersebut. Perangkat router yang menjalankan routing protokol seperti OSPF, apalagi yang sudah terbagi-bagi menjadi beberapa area, sangat membutuhkan kekuatan processing dan memory.

Jika Anda menerapkan OSPF pada router yang salah, maka kinerjanya tidak akan efektif dan malah membuat performa jaringan menjadi jelek. Untuk itu, sebelum mengonfigurasi dan menerapkannya dalam jaringan Anda, telitilah lebih dahulu apakah router Anda memiliki processor dan memory yang cukup kuat untuk itu. Apakah *operating system* router Anda memiliki fitur-fitur OSPF yang ada butuhkan, dan banyak lagi hal yang harus diteliti. Jangan sampai setelah berjalan baru diselidiki kebutuhan dan kelemahannya. 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.

Network administrator harus menemukan cara untuk memblokir akses jaringan yang tidak diinginkan, sementara pada saat yang sama memperbolehkan akses yang tepat.

Gunung Sarjono

ACL: Kebebasan dalam Mengontrol Jaringan

Meskipun *tool* keamanan, seperti *password* dan perangkat pengaman fisik membantu, mereka sering kali kurang fleksibel dalam memfilter *traffic* dan penyediaan kontrol tertentu yang dibutuhkan administrator. Sebagai contoh, network administrator mungkin ingin memperbolehkan akses user ke Internet, tetapi tidak mau user luar telnet ke dalam LAN. Router mempunyai kemampuan memfilter traffic, seperti memblokir akses Internet, dengan *access control list* (ACL). ACL merupakan kumpulan urutan perintan *permit* atau *deny* yang dipergunakan pada alamat atau protokol *upper-layer*.

Apakah ACL?

ACL merupakan daftar instruksi yang Anda buat pada router. Daftar tersebut memberitahu router paket mana yang harus diterima dan paket mana yang harus ditolak. Penerimaan dan penolakan bisa berdasarkan kondisi tertentu, misalnya alamat asal, alamat tujuan, dan nomor port. ACL memungkinkan Anda mengatur traffic dan memeriksa paket tertentu. Semua traffic yang melalui router diuji terhadap kondisi tertentu yang menjadi bagian dari ACL. ACL bisa untuk semua protokol jaringan, misalnya Internet Protocol (IP) dan Internetwork Packet Exchange (IPX). ACL bisa dibuat untuk mengontrol akses ke suatu jaringan atau subnet. Sebagai contoh, pada *PC Media*, ACL bisa digunakan untuk mencegah redaksi memasuki jaringan administrasi.

ACL harus dibuat per protokol. Dengan kata lain, Anda harus membuat ACL untuk setiap protokol pada *interface* jika ingin mengontrol arus traffic pada interface tersebut. (Perlu dicatat bahwa beberapa protokol menyebut ACL sebagai filter.) Sebagai contoh, jika router menggunakan IP, AppleTalk, dan IPX, Anda perlu membuat paling sedikit tiga ACL. ACL dapat digunakan sebagai alat untuk mengontrol jaringan dengan memberikan kebebasan untuk memfilter paket yang mengalir ke atau dari router.

ACL harus dimasukkan secara berurutan, Anda tidak bisa menghapus pernyataan secara terpisah setelah mereka dimasukkan. Anda bisa membuat ACL secara terpisah baru kemudian meng-*copy*-nya ke dalam router. Untuk meng-copy ACL, misalnya dari TFTP server, buat ACL pada TFTP dan simpan file sebagai teks biasa (ASCII). Kemudian, dari router, gunakan perintah untuk meng-copy ACL ke router Anda. Terakhir, simpan ACL ke NVRAM router. Perintah pertama dari ACL yang di-copy akan menimpa ACL sebelumnya selain itu aturan yang baru akan ditambahkan ke bagian akhir ACL tersebut.

Jika Anda telnet ke dalam router dan membuat *access list*, Anda nanti bisa saja diblokir dari router. Untuk menghindari itu, gunakan perintah yang akan me-*restart* router dan me-*load start-up config* tanpa ACL yang memblokir akses.

Mengapa Menggunakan ACL?

Ada banyak alasan untuk membuat ACL. Sebagai contoh, ACL dapat digunakan untuk membatasi traffic jaringan dan meningkatkan kinerja jaringan. Misalnya, ACL dapat membuat paket tertentu supaya diproses oleh router sebelum traffic lain, berdasarkan protokol. Ini disebut *queuing*, yang memastikan bahwa router tidak akan memproses paket yang tidak diperlukan. Hasilnya, queing membatasi traffic jaringan dan mengurangi kemacetan jaringan. ACL dapat Memberikan kontrol terhadap traffic jaringan. Sebagai contoh, ACL dapat melarang atau mengurangi update routing. Larangan ini digunakan untuk membatasi informasi tentang suatu jaringan supaya tidak disebarkan melalui jaringan.

ACL juga dapat memberikan pengamanan (tingkat dasar) untuk akses jaringan. Sebagai contoh, ACL dapat memperbolehkan satu *host* mengakses suatu bagian jaringan Anda dan mencegah host lain mengakses bagian yang sama. Host A diperbolehkan untk mengakses jaringan SDM, dan Host B tidak boleh mengakses jaringan SDM. Jika Anda tidak membuat ACL pada router, semua paket yang dilewatkan melalui router bisa diperbolehkan ke semua bagian jaringan. Terakhir, ACL dapat digunakan untuk memilih jenis traffic yang diteruskan atau diblokir pada router. Sebagai contoh, Anda bisa memperbolehkan e-mail, tetapi pada saat yang sama memblokir semua telnet.

MEMBUAT ACCESS LIST

■ Perintah berikut memfilter traffic dengan standard IP access-list 1

```
Router(config-if)#ip access-group 1 in
```

Perintah berikut memfilter traffic keluar dengan standard IP access-list 1

```
Router(config-if)#ip access-group 1 out
```

Jika arah filter (masuk atau keluar) tidak disebutkan, secara defaut filter menggunakan *outbound*. Suatu interface tidak bisa mempunyai beberapa inbound atau beberapa outbound ACL pada dirinya. Beberapa daftar bisa digunakan jika daftar untuk protokol berbeda. ACL mengikuti aturan berikut:

- Router memberlakukan daftar secara berturut-turut sesuai dengan urutan yang Anda masukkan ke dalam router.
- Router memberlakukan daftar ke paket secara berturut-turut, mulai dari atas ke bawah, per baris.
- Paket hanya diproses jika cocok dan kemudian mereka diperlakukan sesuai dengan kriteria yang terdapat dalam pernyataan ACL.
- Daftar secara implisit selalu diakhiri dengan deny. Router mengabaikan semua paket yang tidak cocok dengan semua pernyataan ACL.
- ACL yang diberlakukan pada suatu interface harus berupa filter traffic inbound atau outbound.
- Hanya satu daftar, per protokol, per arah yang dibisa diberlakukan pada suatu interface.

Aturan ACL

ACL harus dibuat secara berurutan dan selalu diakhiri dengan pernyataan *deny* (penolakan). Karena semua traffic yang yang tidak secara eksplisit diperbolehkan pada ACL akan diblokir, menggunakan perintah acces-list [list #] pada bagian akhir ACL akan memperbolehkan traffic lainnya yang tidak diblokir oleh pernyataan deny untuk melewati interface. Inilah mengapa Anda tidak bisa menambahkan aturan baru ke ACL, semua pernyataan yang ditambahkan sesudah permit any atau perintah deny tidak akan diperiksa. Paket hanya akan diperiksa oleh ACL jika cocok dengan suatu pernyataan.

Pada baris pertama Anda harus memasukkan pernyataan yang kemungkinan besar menemukan paket yang cocok, ini akan mengurangi proses yang tidak perlu dan menghemat waktu CPU. Untuk menghapus ACL gunakan perintah no access-list [list #]. Perintah ini akan menghapus seluruh ACL. Jika Anda tidak terlebih dulu menghapus ACL, semua baris baru akan ditambahkan ke bagian akhir yang lama. Setelah membuat ACL, Anda harus memberlakukan mereka ke interface supaya mereka dapat memfilter traffic. Mereka bisa berupa filter keluar atau masuk.

CONTOH STANDARD IP ACCESS LIST

```
Router(config)#access-list 1 deny host 192.168.1.4
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
Router(config)#int e0
Router(config-if)#ip access-group 1 out
```

Contoh ACL pada router Cisco di atas membolehkan traffic dari 192.168.1.4 masuk ke router, tetapi access list melarangnya keluar dari interface Ethernet 0. Pernyataan deny menggunakan wildcard mask default 0.0.0.0 (misalnya semua bit signifikan dan hanya berlaku untuk satu host). 0.0.0.0 255.255.255.255 bisa digantikan dengan any. Daftar tersebut dihubungkan dengan outbound salah satu interface. Ini akan mencegah host supaya tidak diblokir dari jaringan lain karena traffice dari 192.168.1.4 boleh masuk ke router dan dipindahkan ke jaringan lain pada interface lain selain Ethernet 0. Anda harus menghubungkan standard IP access list sedekat mungkin dengan jaringan tujuan, atau Anda secara tidak sengaja bisa memblokir akses ke suatu bagian jaringan Anda.

Jenis Access List.

JENIS ACCES LIST	NOMOR
Standard IP Access List	1-99
Extended IP Access List	100-199
Standard IPX Access List	800-899
Extended IPX Access List	900-999
IPX SAP Filter	1000-1099

CONTOH STANDARD IPX ACCESS LIST

Contoh ACL pada router Cisco berikut menolak jaringan IPX 500 dari jaringan IPX 200 pada inbound Ethernet 0 dan kemudian membolehkan semua yang lain. ACL ini harus dihubungkan sedekat mungkin ke jaringan 500 untuk mengurangi traffic jaringan. -1 sama seperti perintah any pada IP, yang berlaku untuk semua host.

```
Router(config)#access-list 800 deny 500 200
Router(config)#access-list 800 permit -1 -1
Router(config)#int e0
Router(config-if)#ipx access-group 800 in
```

CONTOH EXTENDED IP ACCESS LIST

Contoh ACL pada router Cisco berikut akan memblokir akses 192.168.1.10 ke TCP port www (http[80]) pada host 192.168.2.2. Kata host merupakan singkatan untuk wildcard mask 0.0.0.0. Karena extended IP access list menggunakan alamat tujuan, list harus dihubungkan sedekat mungkin ke asal untuk mengurangi traffic yang tidak perlu pada jaringan.

```
Router(config)#access-list 100 deny tcp host 192.168.1.10
host 192.168.2.2 eq www
Router(config)#access-list 100 permit ip any any
Router(config)#int e0
Router(config-if)#ip access-group 100 in
```

CONTOH EXTENDED IPX ACCESS LIST

-1 untuk semua protokol atau jaringan IPX. Contoh ACL pada router Cisco berikut menolak akses semua protokol (-1) dan semua socket (0) dari jaringan 500 ke jaringan IP 200 (juga semua socket). Access list ini harus dihubungkan ke inbound interface di mana jaringan IPX 500 berada. Ini akan mengurangi traffic jaringan dan menghemat tenaga router.

```
Router(config)#access-list 900 deny -1 500 0 200 0
Router(config)#access-list 900 permit -1 -1 0 -1 0
Router(config)#int e0
Router(config-if)#ipx access-group 900 in
```

CONTOH IPX SAP FILTER

Perintah pada router Cisco berikut menolak semua SAP advertisement dari jaringan 200, tetapi membolehkan update ke semua bagian jaringan yang lain.

```
Router(config)#access-list 1001 deny 200 0
Router(config)#access-list 1001 permit -1 0
```

Untuk menghubungkan SAP filter ke inbound interface, gunakan perintah:

```
Router(config)#int e0
Router(config-if)#ipx input-sap-filter 1001
```

Atau untuk menghubungkan access list ke outbound interface, gunakan perintah:

```
Router(config)#int e0
Router(config-if)#ipx output-sap-filter 1001
```

Perintah di atas akan memblokir semua advertisement dari jaringan 200 supaya tidak dilewatkan ke router lain pada jaringan.

Standard IP Access List

Standard IP access list memfilter traffic jaringan berdasarkan alamat IP asal. Dengan standard access list, Anda dapat memfilter traffic berdasarkan alamat IP, subnet, atau alamat jaringan host. Untuk membuat standard IP access list, pertama Anda harus membuat access list dan kemudian menghubungkannya ke suatu interface.

Standard IPX Access List

Standard IPX Access List sama dengan standard IP access list, hanya saja mereka dapat memfilter berdasarkan alamat atau jaringan asal dan tujuan.

Extended IP Access List

Extended IP access list dapat memfilter berdasarkan alamat IP asal, alamat IP tujuan, jenis protokol, aplikasi tujuan dan nomor port asal, sementara standard IP access list hanya dapat memfilter alamat asal. Anda juga bisa membuat extended IP access list dengan daftar dan menghubungkannya ke suatu interrface.

Extended IPX Access List

Extended IPX access list memungkinkan Anda untuk memfilter berdasarkan alamat jaringan atau node asal dan tujuan, jenis protokol IPX, dan IPX socket.

IPX SAP Filter

IPX SAP filter membatasi traffic SAP untuk mengontrol *resource* mana pada jaringan IPX yang akan terlihat oleh IPX client. Ini memungkinkan Anda untuk membatasi *advertisement* dari suatu server atau service ke bagian tertentu jaringan IPX. Karena SAP advertisement merupakan *broadcast*, membatasi mereka dapat mengurangi traffic jaringan. IPX SAP filter juga bisa digunakan untuk memblokir advertisement server antarbagian yang terpisah. ■

LEBIH LANJUT

- **http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacls.htm**
- **http://www.cisco.com/warp/public/105/acl_wp.html**

Kali ini kita akan melihat ide di belakang Linux dan menghilangkan beberapa mitos tentang *operating system open source*.

Gunung Sarjono

Langkah Pertama pada Linux

Linux dimulai sebagai proyek seorang murid di Helsinki bernama **Linus Torvalds**. Visinya adalah menciptakan suatu versi dari Unix yang didasarkan pada usaha kolaboratif dan terdiri dari kode *open source*. Hasil dari visi ini adalah kernel Linux, yang merupakan inti dari semua distribusi yang tersedia. Secara sederhana, Linux merupakan *operating system* yang sama dengan Windows: software dasar yang Anda butuhkan supaya PC Anda dapat bekerja dan digunakan.

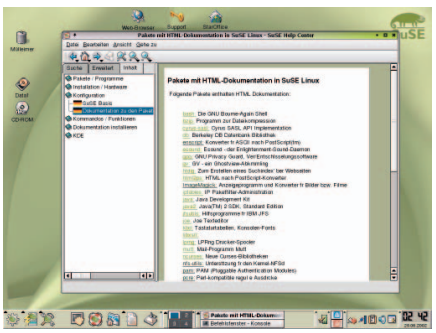
Bagi beberapa kelompok, Linux merupakan jalan untuk menantang dominasi Microsoft pada pasar PC. Kita tidak lagi terbelenggu dengan tingkah **Bill Gates**. Malah, kita bebas memilih, bahkan pada waktu memilih OS. Bagi yang lain, Linux tidak berguna, rasa penasaran para teknisi, sesuatu yang dikerjakan sembarangan pada PC tua oleh murid-murid, orang yang sangat aneh dan pembenci Microsoft yang kuat. Kenyataannya, tentu ada di tengah-tengah, tetapi sebelum kita mulai dengan pro dan kontra, mari kita lihat faktanya.

Fakta

Fakta nomor satu adalah Linux merupakan *operating system* yang utuh dan dapat dipakai, dalam banyak hal lebih dari cukup untuk menyaingi Windows dan bagi banyak orang bisa menggantikannya. Linux merupakan penyelamat dunia bebas. Pada kenyataannya, Linux merupakan operating system yang dapat melakukan hampir semua yang bisa dilakukan Windows dan dalam beberapa hal sedikit lebih baik dibanding produk Microsoft. Perbedaan utama antara Linux dan Windows adalah Linux itu gratis (*free*). Linux tidak hanya alternatif Windows yang bebas biaya, *source code*-nya juga betul-betul terbuka untuk dilihat dan diubah oleh umum. Bandingkan itu dengan Windows, di mana source code untuk OS itu dijaga ketat sebagai rahasia dagang. Semua programer di seluruh dunia bebas untuk mengubah setiap bagian Linux, sepanjang mereka merilis perubahan atau penambahan yang mereka lakukan kepada umum. Inilah yang disebut open source, dan ini merupakan istilah yang akan sering Anda dengar pada waktu belajar tentang Linux.

Namun, jika semua programer dapat mengubah OS, bukankah itu berarti kita membuka diri terhadap segala jenis masalah yang mungkin terjadi? Dapatkah semua orang menambahkan kode yang bisa menghancurkan data, atau meng-e-mail file pribadi kita ke seluruh dunia tanpa sepengetahuan dan seizin kita?

Tampilan *desktop* Linux Mandrake.



Tampilan *desktop* Linux SUSE.

PARTISI LINUX DAN WINDOWS

Salah satu perbedaan utama antara Linux dan Windows adalah cara pembuatan dan pengaturan sistem file. Windows akan menginstalasi dan menjalankan semuanya dari satu drive atau partisi, sementara Linux tidak. Pertama, Linux menggunakan format sistem file yang berbeda dengan sistem FAT32 dan NTFS yang digunakan oleh Windows. Sistem file *default* Linux bernama Ext3. Harddisk yang diformat menggunakan Ext3 aslinya tidak dapat dibaca oleh Windows, tetapi ada driver pihak ketiga yang memungkinkan akses ke mereka.

Linux juga mempunyai cara yang berbeda dengan Windows dalam menangani partisi harddisk. Instalasi Linux standar membutuhkan beberapa partisi yang digunakan untuk menyimpan bagian sistem yang berbeda. Sebagai contoh, Windows menyimpan file swap virtual memoy sebagai file tersembunyi pada boot drive, sementara Linux membutuhkan partisi terpisah. Bagian utama dari sistem membutuhkan partisi lain, biasanya partisi root. Terakhir, semua file user juga disimpan pada partisi lain, disebut dengan partisi *home*.

Meskipun mungkin, itu belumlah terjadi dan lingkungan komunitas Linux global membuat kekhawatiran tersebut sangat tidak relevan. Sementara Microsoft mengontrol dan mengawasi Windows, seluruh dunia menjaga Linux.

Ada sekelompok programer yang bergabung bersama dengan ide membuat Linux versi modifikasi mereka sendiri. Beberapa ingin mengarahkan Linux versi mereka kepada user tertentu misalnya penggunaan server murni bukan untuk penggunaan desktop, sementara yang lain ingin membuat ulang Linux sesuai kebutuhan mereka sendiri. Ini memperluas konsep dari distribusi atau *distro* Linux, istilah lain yang akan banyak Anda dengar.

Permainan Nama

Karena setiap kelompok membuat Linux sendiri, mereka memberikannya sebuah nama. Inilah sebabnya Anda akan melihat banyaknya variasi Linux yang berbeda dan membingungkan, misalnya Debian, Red Hat, SUSE, dan sebagainya. Masing-masing mempunyai keunikan dan fitur positif sendiri. Memilih suatu versi Linux tidak berbeda dengan memilih es krim; hanya masalah selera. Pada kesempatan berikutnya, kita akan melihat distribusi besar dan juga yang kurang terkenal tetapi lebih spesifik. Versi Linux yang dibuat khusus untuk anak-anak merupakan salah satu contoh yang perlu dinantikan.

Pro dan Kontra

Jadi, keuntungan Linux adalah gratis, mempunyai banyak aplikasi yang tersedia untuknya, mempunyai *support* dari vendor distribusi dan komunitas user, dan tuntutan hardware yang lebih rendah dibanding Windows. Jadi, apakah kerugiannya?

Pertama, adanya beragam jenis Linux bisa menjadi kelemahan tetapi bisa juga menjadi nilai tambah. Dengan banyaknya distribusi yang ada, bagaimana Anda bisa memilih? Masing-masing mempunyai kawan dan lawan sendiri. Kedua adalah *software* dan *hardware* yang mendukung aplikasi Windows tidak akan berjalan pada Linux, meskipun banyak yang bisa dibujuk. Hasilnya, Anda tidak bisa begitu saja menginstalasi Microsoft Office atau Adobe Photoshop dan menggunakannya. Sangat sedikit perusahaan software yang membuat versi Linux dari produk mereka dan Anda akan sangat sulit mendapatkan mereka di pasaran.

Berita baiknya adalah dengan sedikit pengecualian ada beberapa program ekivalen yang tersedia dan banyak di antaranya mempertahankan kompatibilitas penuh dengan Windows. Terlebih lagi, banyak dari mereka juga bebas digunakan. Ada paket office suite, video editor, CD burning suite, 3D modeller, art, dan sebagainya.

User dan Administrator

Linux secara teguh memberlakukan konsep *user account* yang terbatas dan account administrator yang mahakuasa. Jika menggunakan Windows 2000 atau XP, Anda tentu sudah tidak asing lagi dengan konsep administrator dan user, dan juga fakta bahwa masing-masing user PC Anda mempunyai *login account* sendiri. Ide ini cukup baru dalam dunia Windows. Sebagai contoh, Windows 98 hanya mempunyai sedikit kemampuan multiuser dan sama sekali tidak mempunyai opsi sekuriti yang ditawarkan oleh Windows XP.

Linux berbeda dalam hal ini dan menganut konsep administrator dan user pada berbagai tingkat yang berbeda. Sebagai contoh, bacalah setiap dokumentasi Linux dan Anda akan melihat disebutkannya kata "root" secara rutin. Dalam istilah Linux, root merupakan nama yang diberikan kepada administrator absolut dari sistem Linux. Root merupakan nama sebenarnya dari user yang mempunyai akses penuh terhadap semua aspek instalasi Linux dan dapat melakukan semua hal pada semua file.

Masing-masing user pada sistem juga mempunyai username, password, dan home directory sendiri. User Linux biasa tidak akan pernah mempunyai hak yang sama dengan user root—dikenal mempunyai akses root—karena faktor keamanan.

Dukungan Hardware

Dukungan hardware untuk Linux secara umum sangat baik sekarang ini, dan komponen yang paling asing pada PC Anda akan dikenali dan dikonfigurasi pada waktu Linux diinstalasi. Banyak *distro* yang datang dengan tool hebat untuk mengenali dan mengonfigurasi hardware baru pada waktu Anda menginstalasinya, membuat Anda merasa sama dengan Windows. Meskipun begitu, beberapa hardware akan selalu menjadi masalah, atau mereka yang ada sulit untuk diinstalasi, sering kali harus diinstalasi secara manual melalui *command-line*.

Namun, jangan biarkan ini menangguhkan niat Anda. Linux bisa menjadi alternatif Windows yang menarik dan menyenangkan, dan dengan sedikit usaha keduanya bisa berada pada satu PC yang sama. Berikutnya, kita akan melihat langkah pertama dalam mempersiapkan sistem Anda untuk intalasi Linux. Sampai jumpa lagi. ■

LEBIH LANJUT

- **http://www.clockwatchers.com/linux_main.html**
- **http://www.linux-directory.com/newbie**
- **http://www.linuxlots.com/~jam**

Pada waktu **Julius Caesar** mengirim pesan kepada jenderalnya, ia tidak mempercayai si kurir. Jadi ia mengganti huruf A dengan D, B dengan E, dan seterusnya. Hanya yang tahu aturan "pergeseran 3" yang dapat membaca pesannya.

Gunung Sarjono

PGP Sebagai Penanda Digital

PGP (disebut juga "*Pretty Goog Privacy*") merupakan program komputer yang mengenkripsi (mengacak) dan mendekripsi (menyusun) data. Sebagai contoh, PGP dapat mengenkripsi "Andre" menjadi "457mRT%$354." Komputer Anda dapat menyusun kembali campuran karakter acak tersebut menjadi "Andre" jika Anda mempunyai PGP.

PGP memberikan privasi kepada file dan e-mail Anda. Ia melakukannya dengan enkripsi sehingga tidak ada seorang pun kecuali yang dituju yang dapat membacanya. Pada waktu dienkripsi, e-mail terlihat seperti campuran karakter acak yang tidak berarti. PGP telah membuktikan dirinya cukup mampu dalam melawan berbagai bentuk analisis yang dilakukan untuk membaca teks yang dienkripsi.

PGP juga dapat digunakan sebagai *digital signature* (penanda digital) pada pesan tanpa mengenkripsinya. Ini biasanya digunakan pada *public posting*, di mana Anda tidak ingin menyembunyikan apa yang Anda katakan, tetapi Anda ingin supaya orang lain yakin bahwa pesan itu dari Anda. Setelah penanda digital dibuat, tidak mungkin untuk mengubah pesan atau *signature* tanpa terdeteksi oleh PGP.

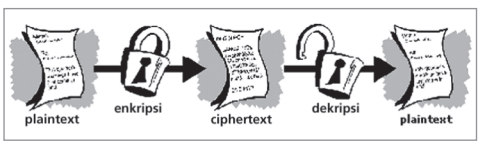
Meskipun PGP terlihat (dan menurut banyaknya penggunanya) mudah digunakan, Anda bisa stres dibuatnya. Anda harus betul-betul mengenal berbagai opsi pada PGP sebelum menggunakannya untuk mengirim pesan penting. Sebagai contoh, memberi perintah *pgp -sat <filename>* hanya akan menandai dan melapisi pesan dengan kode ASCII, ia tidak akan mengenkripsi pesan. Meskipun *output*-nya tampak seperti terenkripsi, sebenarnya tidak (kode ASCII-lah yang tampak demikian). Semua orang bisa melihat pesan yang asli dengan perintah *pgp <encryptedfilename>*.

Enkripsi dan Dekripsi

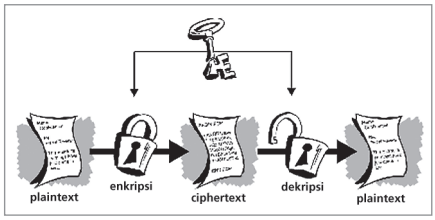
Data yang dapat dibaca dan dimengerti tanpa cara tertentu disebut *plaintext* atau *cleartext*. Metode untuk menyamarkan plaintext sedemikian rupa untuk menyembunyikan isinya disebut enkripsi. Mengenkripsi plaintext menghasilkan karakter acak yang tidak dapat dibaca yang disebut *ciphertext*. Anda menggunakan enkripsi untuk memastikan informasi tersebut tersembunyi dari semua orang yang tidak berkepentingan, termasuk mereka yang dapat melihat data yang terenkripsi. Proses mengubah *chipertext* ke *plaintext* asli disebut dekripsi.

Siapa yang Membuat PGP?

Philip Zimmermann merupakan orang yang membuat program awal. Phil, pahlawan bagi banyak aktivis proprivasi, bekerja sebagai konsultan sekuriti komputer di Boulder, Colorado pada waktu itu. Programer lain di seluruh dunia membuat versi PGP dan/atau *shell* selanjutnya. Versi PGP lanjutan dibuat oleh sebuah perusahaan di California bernama Network Associates, yang membeli perusahaan sebelumnya, didirikan oleh Zimmermann, bernama PGP Inc. Penggabungan perusahaan merupakan hal biasa di Amerika. Siapa yang tahu pihak selan-



Enkripsi dan dekripsi.



Enkripsi biasa.

jutnya yang akan mengontrol PGP pada waktu membaca artikel ini?

Apakah Cryptography?

Cryptography merupakan ilmu yang menggunakan matematika untuk meng-enkripsi dan mendekripsi data. Dengan cryptography, Anda dapat menyimpan informasi penting atau mengirimkannya melalui jaringan yang tidak aman (seperti Internet) sehingga data tersebut tidak dapat dibaca oleh siapapun kecuali penerima yang dimaksud.

Sementara cryptography merupakan ilmu pengamanan data, *cryptanalysis* merupakan ilmu menganalisis dan memecahkan komunikasi yang aman. *Cryptanalysis* yang klasik melibatkan kombinasi pemikiran analitis, penggunaan tool matematis, pencarian pola, kesabaran, dan keberuntungan. Pada *crypanalyst* juga disebut *attacker* (penyerang). Cryptology mencakup cryptography dan crypanalysis.

Bagaimana Cryptography Bekerja?

Algoritma *cryptographic* atau *chiper*, merupakan fungsi matematis yang digunakan dalam proses enkripsi dan dekripsi. Algoritma cryptographic dikombinasikan dengan *key* (kunci)—suatu kata, angka, atau frase—untuk mengenkripsi *plaintext*. Plaintext yang sama dienkripsi ke ciphertext lain dengan key yang berbeda. Keamanan dari data yang terenkripsi seluruhnya bergantung kepada dua hal: kekuatan algoritma cryptographic dan kerahasiaan key.

Algoritma cryptographic, plus key, dan semua protokol yang membuatnya bekerja membuat suatu *cryptosystem*. PGP merupakan suatu cryptosystem. Pada cryptography biasa, disebut juga enkripsi *secret-key* atau *symetric-key*, satu key digunakan untuk enkripsi dan dekripsi. Data Encryption Standard (DES) merupakan salah satu contoh dari cryptosystem biasa.

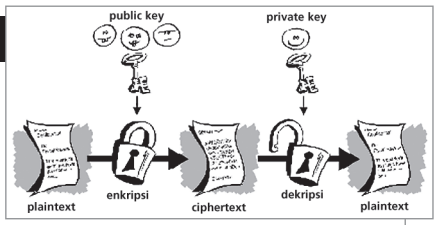
Siapa yang Menggunakan Enkripsi PGP?

Orang-orang yang menghargai privasi menggunakan PGP. Politikus yang menjalankan kampanye pemilihan, pembayar pajak yang menyimpan data, terapis yang melindungi file klien, wiraswasta yang menjaga rahasia dagang, jurnalis yang melindungi sumbernya, dan mereka yang mencari pasangan merupakan beberapa dari orang-orang yang menggunakan PGP untuk menjaga supaya file komputer dan e-mail mereka tetap rahasia.

Kalangan bisnis juga menggunakan PGP. Misalkan Anda seorang manajer perusahaan dan Anda perlu meng-e-mail seorang karyawan mengenai kinerjanya. Anda mungkin diharuskan oleh hukum untuk menjaga supaya e-mail itu rahasia. Misalkan Anda seorang *sales* dan harus berkomunikasi dengan kantor cabang tentang daftar pelanggan Anda melalui jaringan komputer publik. Anda mungkin diharuskan perusahaan Anda dan hukum untuk menjaga supaya daftar tetap rahasia. Ada beberapa alasan mengapa kalangan bisnis menggunakan enkripsi untuk melindungi pelanggan, karyawan, dan mereka sendiri.

PGP juga membantu mengamankan transaksi keuangan. Sebagai contoh, Electronic Frontier Foundations menggunakan PGP untuk mengenkripsi nomor

PUBLIC KEY CRYPTOGRAPHY



Enkripsi public key.

PGP merupakan salah satu jenis *public key cryptography*. Public key cryptography merupakan model asimetris yang menggunakan sepasang kunci untuk enkripsi: *public key*, yang mengenkripsi data, dan pasangannya *private* atau *secret key* untuk mendekripsi. Semua orang (bahkan mereka yang belum pernah Anda temui) yang mempunyai public key Anda dapat mengenkripsi informasi yang hanya dapat dibaca oleh Anda. Berikut adalah contoh *public key*:

```
—BEGIN PGP PUBLIC KEY BLOCK—
Version: 5.0

mQCNAi44C30AAAEEAL1r6ByIvuSAvOKIk9ze9yCK+ZPPbRZrpXIRFBbe+U8dGPMb
9XdJS4L/cy1fXr9R9j4EfFsK/
rgHV6i2rE83LjOrmsDPRPSaizz+EQTIZi4AN99j
iBomfLLZyUzmHMoUoE4shrYgOnkc0u101ikhieAFje77j/F3596pT6nCx/
9/AAUR
tCRBbmRyZSBCYWNhcmQgPGFiYWNhcmRAd2VsbC5zZi5jYS51cz6JAFUCBRAuOA6O
7zYZz1mqos8BAXr9AgCxCu8CwGZRdpfSs65r6mb4MccXvvfxO4TmPi1DKQj2FYHY
jwYONk8vzA7XnE5aJmk5J/dChdvfIU7NvVifV6AF
=GQv9
—END PGP PUBLIC KEY BLOCK—
```

Misalkan public key di atas milik Anda dan Anda meng-e-mail-nya kepada kami. Kami bisa menyimpan public key Anda dalam program PGP kami dan menggunakan public key Anda untuk mengenkripsi pesan yang hanya bisa dibaca oleh Anda. Salah satu keindahan *public key cryptography* adalah Anda dapat memberikan public key Anda sama seperti Anda memberikan nomor telepon Anda. Jika kami mempunyai nomor telepon Anda, kami bisa menelpon Anda; namun, kami tidak dapat menjawab telepon Anda. Sama juga, jika kami mempunyai public key Anda, kami bisa mengirim e-mail kepada Anda; tetapi, kami tidak bisa membaca e-mail Anda. Konsep public key ini mungkin terdengar misterius pertamanya. Namun, menjadi sangat jelas pada waktu Anda menggunakan PGP selama beberapa waktu.

BAGAIMANA MEMPUBLIKASIKAN PUBLIC KEY SAYA?

PGP dan GPG versi terbaru secara otomatis akan berhubungan dengan key server jika Anda terhubung ke Internet dan Anda mengonfigurasinya untuk itu. Untuk menyebarkan key secara manual, kirim e-mail dengan subjek "help" ke salah satu alamat berikut untuk mengetahui bagaimana menggunakan mereka:

- pgp-public-keys@keys.pgp.net
- pgp-public-keys@keys.de.pgp.net
- pgp-public-keys@keys.no.pgp.net
- pgp-public-keys@keys.uk.pgp.net
- pgp-public-keys@keys.us.pgp.net

account iuran anggota, sehingga anggota itu bisa membayar iuran melalui e-mail.

Bukankah Komputer dan E-mail Sudah Aman?

File komputer Anda (kecuali dienkripsi) dapat dibaca oleh semua orang yang bisa mengakses komputer Anda. E-mail terkenal tidak aman. E-mail berjalan melalui banyak komputer. Orang yang menjalankan komputer tersebut bisa membaca, meng-*copy*, dan menyimpan e-mail Anda. Banyak kompetitor yang sangat ingin menangkap e-mail. Mengirim e-mail bisnis, hukum, dan pribadi melalui komputer bahkan kurang rahasia dibanding mengirim materi yang sama melalui kartu pos. PGP merupakan salah satu "amplop" aman yang menjaga orang-orang, kompetitor, dan kriminal supaya tidak menyerang Anda.

Mengapa Saya Harus Mengenkripsi E-mail? Saya Tidak Melakukan Sesuatu Yang Ilegal!

Alasan mengapa harus mengenkripsi e-mail sama dengan alasan mengapa Anda tidak menulis semua pesan Anda di belakang kartu pos. E-mail sebenarnya jauh kurang aman dibanding sistem pos. Pada kantor pos, surat Anda ditangani oleh pekerja pos. Coba lihat bagian kepala semua e-mail yang Anda terima dan Anda akan melihat bahwa mereka melalui sejumlah *nodes* pada waktu menuju ke Anda. Semua orang pada nodes tersebut mempunyai kesempatan untuk menyusup, juga semua sistem yang dapat mendengarkan komunikasi antara node tersebut. Enkripsi sama sekali tidak untuk menunjukkan aktivitas ilegal. Ia hanya dimaksudkan untuk menjaga supaya yang pribadi tetap pribadi.

Saya Tidak Menyembunyikan Apa-Apa. Mengapa Saya Membutuhkan Privasi?

Coba sebutkan orang yang tidak mempunyai rahasia dari keluarga, tetangga, atau rekan kerjanya, dan kami akan menunjukkan orang yang betul-betul suka sekali menceritakan rahasia-rahasianya atau betul-betul pendiam. Coba sebutkan bisnis yang tidak mempunyai perdagangan tersembunyi atau catatan rahasia, dan kami akan menunjukkan bisnis yang sangat tidak berhasil. Privasi, kebebasan, kerahasiaan, dan kebijaksanaan merupakan tanda-tanda suatu peradaban.

Saya Mendengar Bahwa Enkripsi Dilarang karena Pelaku Kriminal Menggunakannya untuk Menghindari Deteksi. Apakah Ini Benar?

Banyak pemerintahan, perusahaan, dan badan penegak hukum yang menggunakan enkripsi untuk menutupi kegiatan mereka. Benar, beberapa pelaku kriminal juga menggunakan enkripsi. Namun, pelaku kriminal cenderung menggunakan mobil, sarung tangan, dan topeng untuk menghindari penangkapan. PGP merupakan "enkripsi untuk orang banyak." PGP memberikan hak privasi kepada warga negara yang diklaim pemerintah dan perusahaan dibutuhkan untuk mereka sendiri.

Seberapa Amankah PGP?

Selama beberapa tahun, kode PGP dipublikasikan supaya ahli sekuriti dapat memeriksa adanya "*back door*" (jalan tersembunyi untuk membobol pesan PGP). Mungkin pemerintah dapat meng-"hancurkan"-kan pesan PGP dengan menggunakan superkomputer dan/atau orang sangat pintar. Kami tidak tahu. Yang pasti ada tiga fakta. Pertama, *cryptographer* dan ahli komputer ternama belum berhasil membobol PGP. Kedua, siapapun yang membuktikan bahwa ia dapat memecahkan PGP akan cepat mendapatkan ketenaran dalam kelompok *crypto*. Ia akan disambut pada perjamuan dan mendapatkan banyak uang. Ketiga, pengguna PGP di seluruh dunia akan segera menyebarkan berita ini.

Hampir setiap hari, seseorang mengirim pemberitahuan seperti "PGP Dibobol oleh Remaja dari Omaha." Jangan termakan oleh klaim tersebut. Dunia crypto tidak memberi perhatian terhadap paranoid, provokator, dan alien UFO. Sejauh ini, tidak ada yang secara umum menunjukkan kemampuan untuk menaklukan PGP.

Apakah PGP Sah di Amerika Serikat?

Ya. Namun, Anda tidak diperbolehkan mengekspor PGP ke luar Amerika Serikat tanpa persetujuan pemerintah. Jangan pernah memikirkan hal itu! Untuk berkomunikasi dengan teman, misalnya di Inggris, mintalah teman Anda untuk mendapatkan PGP dari luar Amerika Serikat.

Apakah PGP Sah di Luar Ameriksa Serikat?

Legalitas PGP bervariasi dari negara ke negara. Plus, hukum di seluruh dunia selalu berubah. Di sebagian besar negara, penggunaan enkripsi tidak melanggar hukum atau paling tidak dibolehkan. Namun, pada beberapa negara aktivitas tersebut bisa membuat Anda dihukum berat! Contoh negara di mana penggunaan enkripsi ilegal adalah Prancis, Iran, Rusia, dan Irak. Anda harus mengecek hukum di mana Anda tinggal.

Apakah Digital Signature PGP?

Misalkan artikel ini ditandai dengan "*digital signature*" PGP kami. Ini memungkinkan orang yang mempunyai

PGP dan public key kami dapat memastikan bahwa ini: 1) Kami *PC Media*, (bukan majalah lain yang berpura-puram menjadi kami) yang menerbitkan artikel ini, dan 2) tidak ada seorang pun yang mengubahnya sejak kami tandai. Signature PGP dapat membantu untuk menandatangani kontrak, mentransfer uang, dan memeriksa identitas seseorang.

Seberapa Sulit Mempelajari PGP?

PGP lebih mudah digunakan daripada, katakanlah, program pengolah kata. Versi Windows terbaru memungkinkan Anda mengenkripsi dan dekripsi file dan e-mail dengan beberapa klik mouse.

Versi PGP Berapa Saja yang Ada Saat Ini?

Ada tiga "jajaran-produk" yang berbeda untuk PGP, yaitu PGP 2.x, PGP 5.x dan lebih tinggi, dan GNU Privacy Guard.

Platform Apa yang Digunakan PGP?

PGP 2.x dan berbagai versinya tersedia dalam berbagai platform, termasuk Microsoft Windows, DOS, f, OS/2, Unix (hampir semua varian), VMS, Atari ST, Acorn RISC OS (Archimedes), Commodore Amiga, EPOC, dan Palm OS. PGP 5.x dan selanjutnya tersedia untuk Microsoft Windows dan Mac OS 8.x/9x. Perlu dicatat untuk PGP 7.x belum mendukung Microsoft Windows XP. GNU Privacy Guard sebagian besar untuk sistem UNIX-like dan dapat bekerja pada GNU/Linux, GNU/Hurd, FreeBSD, OpenBSD, NetBSD, dan berbagai sistem UNIX-like komersial. Ada juga versi *command line* untuk Microsoft Windows.

Apakah Versi PGP Saling Kompatibel?

Secara umum, ya. Sebagai contoh, dokumen yang dienkripsi dengan PGP Windows dapat didekripsi oleh orang yang menggunakan PGP Unix. Anda juga akan menemukan bahwa PGP versi "internasional" juga kompatibel dengan versi "domestik" (Amerika Serikat).

Berapa Biaya untuk PGP?

PGP 2.x dan GNU Privacy Guard tersedia bebas sebagai software *open source* di bawah GNU General Public License dengan tidak ada batasan penggunaan dan tidak perlu biaya (kecuali hak paten IDEA yang perlu Anda pilih untuk memasukkan dukungan untuk itu), sementara PGP 5.x dan lebih tinggi merupakan produk komersial. Network Associates membeli PGP Inc., perusahaan yang dibangun Phill Zimmerman, dan menjual seluruh jajaran produk dengan merk "PGP". PGP e-mail dan enkripsi file yang "asli" bernama PGPMail dan PGPfile.

Perlu dicatat bahwa PGP yang *free* hanya gratis bila digunakan untuk keperluan nonkomersial. Jika Anda perlu menggunakan PGP untuk komersial, Anda harus membeli PGP dari NAI (*http://www.pgp.com*). Versi PGP untuk komersial juga mempunyai keuntungan lain, seperti integrasi dengan aplikasi Windows dan Mac OS, lisensi terbatas untuk mengekspornya ke cabang kantor di luar negeri dan lisensi IDEA.

Key

Key merupakan nilai yang dapat digunakan algoritma *crytographic* untuk menghasilkan *ciphertext* tertentu. Key pada dasarnya hanya merupakan angka yang sangat, sangat, sangat besar. Ukuran key diukur dalam bit; angka yang mewakili key 1024-bit sangat besar sekali. Pada cryptography public key, semakin besar key, semakin aman *ciphertext*.

Namun, tidak ada hubungan antara ukuran public key dan ukuran *secret key* cryptography biasa. Key biasa 80-bit mempunyai kekuatan yang setara dengan public key 1024-bit. Key biasa 128-bit setara dengan public key 3000-bit. Semakin besar key, semakin aman, tetapi algoritma yang digunakan untuk tiap jenis cryptography sangatlah berbeda, seperti apel dengan jeruk.

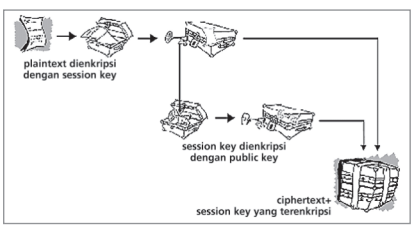
Meskipun public dan private key secara matematis berhubungan, sangat

CARA KERJA PGP

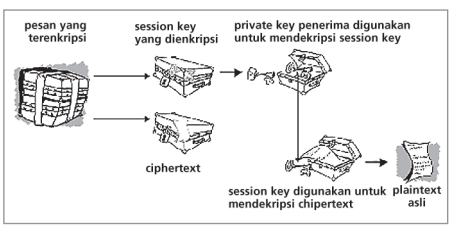
PGP menggabungkan beberapa fitur *cryptography* biasa dan *public key*. PGP merupakan *cryptosystem* campuran. Pada waktu user mengenkripsi *plaintext* dengan PGP, PGP pertama mengompresi plaintext tersebut. Kompresi data menghemat waktu transmisi dan ruang harddisk dan lebih penting, memperketat sekuriti *cryptographic*. Sebagian besar teknik *crypanalysis* memanfaatkan pola yang ditemukan pada plaintext untuk membobol *cipher*. Kompresi mengurangi pola tersebut, sehingga meningkatkan daya tahan terhadap crypanalysis. (File yang terlalu kecil untuk dikompresi atau tidak dapat terkompresi dengan baik tidak dikompresi).

PGP kemudian membuat *session key*, yang merupakan key rahasia yang berlaku hanya satu kali. Key ini merupakan angka acak yang dibuat dari pergerakan acak mouse Anda dan tombol yang Anda tekan. Setelah data dienkripsi, session key kemudian dienkripsi ke public key penerima. Public key ini ditransmisikan bersama *ciphertext* kepada penerima. Dekripsi bekerja sebaliknya. PGP penerima menggunakan private key miliknya untuk membuat session key sementara, yang kemudian digunakan PGP untuk mendekripsi *ciphertext*.

Kombinasi dari dua metode tersebut menggabungkan kenyamanan enkripsi public key dengan kecepatan enkripsi biasa. Enkripsi biasa kira-kira 1000 kali lebih cepat dibanding enkripsi public key. Sebagai gantinya, enkripsi public key memberikan solusi dalam masalah penyebaran key dan transmisi data. Digunakan bersama-sama kinerja dan penyebaran key bisa ditingkatkan tanpa perlu mengorbankan keamanan.



Cara kerja enkripsi PGP.



Cara kerja dekripsi PGP.

BEBERAPA TEMPAT UNTUK MENDAPATKAN PGP

PGP freeware—untuk penggunaan pribadi, nonkomersial

- http://www.pgpi.com/—Tempat terbaik untuk versi terbaru.
- http://web.mit.edu/network/pgp.html—Tempat terpercaya untuk orang Amerika Utara.
- http://cryptography.org/—Tempat kumpulan versi lama dan versi untuk berbagai *platform* bagi orang Amerika Utara.

GNU Privacy Guard—gratis untuk penggunaan nonkomersial

- http://www.gnupg.org/
- http://www.pgpi.com/
- http://cryptography.org/

PGPmail versi komersial

PGPmail sekarang didistribusikan dan didukung oleh PGP Corporation. Kunjungi *http://www.pgp.com/* untuk mengetahui harga, versi, dan *support*-nya. Untuk penggunaan komersial di mana support penting, atau di mana integrasi maksimum dengan Windows juga penting, ini merupakan opsi yang lebih baik. Untuk penggunaan komersial di mana harga murah menjadi pilihan utama dan Anda ingin menggunakan *command line interface*, GNU Privacy Guard (*http://www.gnupg.org*) lebih baik.

sulit untuk membuat private key dengan public key saja; namun, membuat private key selalu dapat dilakukan dengan waktu dan tenaga komputasi yang cukup. Oleh karena itu, sangat penting untuk memilih key dengan ukuran yang tepat; cukup besar supaya aman, tetapi cukup kecil supaya dapat dibuat dengan cepat. Di samping itu, Anda perlu memikirkan siapa saja yang mungkin membaca file Anda, bagaimana mengklarifikasi mereka, berapa lama waktu yang mereka punya, dan *resource* apa yang mereka punya.

Key yang lebih besar secara cryptographic aman untuk waktu yang lebih lama. Jika yang ingin Anda enkripsi perlu disembunyikan selama beberapa tahun, Anda harus menggunakan key yang sangat besar. Tentu saja, siapa yang tahu berapa lama waktu yang diperlukan untuk membuat key Anda menggunakan komputer masa depan yang lebih cepat dan efisien?

Key disimpan dalam bentuk yang terenkripsi. PGP menyimpan key dalam dua file pada harddisk Anda; satu untuk public key dan satu lagi untuk private key. Kedua file ini disebut *keyring*. Pada waktu menggunakan PGP, Anda akan memasukkan public key untuk penerima ke public keyring Anda. Private key Anda akan disimpan dalam private keyring Anda. Jika private key Anda hilang, Anda tidak akan dapat mendekripsi informasi yang terenkripsi dengan key pada ring tersebut.

Bisakah Public Key Dipalsukan?

Secara singkat: tidak secara keseluruhan, tetapi mungkin sebagian. Public key mempunyai empat bagian, masing-masing mempunyai kelemahannya sendiri. Keempat bagian tersebut adalah *user ID*, *key ID*, *signatures*, dan *key fingerprint*. Tidak sulit untuk membuat user ID palsu. Jika user ID pada suatu key berubah, dan key tersebut kemudian dimasukkan ke keyring lain, user ID tersebut akan dilihat sebagai user ID baru dan ia digabungkan ke yang sudah ada. Ini menunjukkan bahwa user ID yang tidak dikenal jangan dipercaya.

Adalah mungkin untuk membuat key dengan key ID tertentu. Key ID hanya 64 bit bagian bawah dari *public key* (tetapi hanya 32 bit yang ditampilkan oleh pgp -kv). Tidak sulit untuk memilih dua bilangan prima yang pada waktu dikalikan mempunyai urutan low-order bit tertentu. Ini memungkinkan dibuatnya key palsu dengan key ID yang sama dengan yang ada. Meskipun begitu, *fingerprint*-nya masih berbeda.

Sekarang ini belum ada metode untuk membuat signature palsu untuk user ID pada key seseorang. Untuk membuat signature buat user ID, Anda memerlukan *secret key* pembuat signature. Signature sebenarnya menandai sebagian user ID, jadi Anda tidak bisa mengcopy signature satu user-ID ke yang lain atau mengubah user ID yang telah ditandai tanpa membuat signature tidak berlaku lagi. Ya, bisa saja membuat public key dengan fingerprint yang sama dengan yang sudah ada, tetapi key tersebut tidak akan mempunyai panjang yang sama jadi mudah untuk diketahui. Biasanya key semacam itu mempunyai panjang yang ganjil.

Bagaimana Mendeteksi Key Palsu?

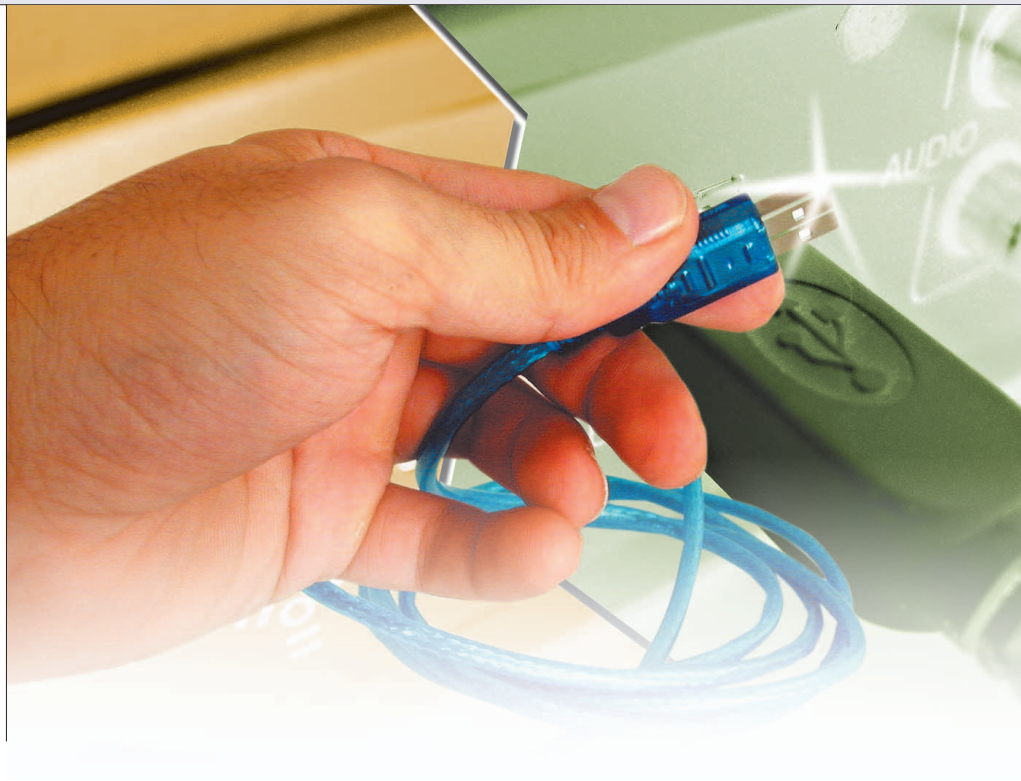
Seperti yang dijelaskan sebelumnya, setiap komponen public key dapat dipalsukan. Namun, tidak mungkin untuk membuat key palsu yang semua komponennya sama. Oleh karena itu, Anda harus selalu memeriksa key ID, *fingerprint*, dan ukurannya pada waktu Anda akan menggunakan key orang lain. Dan pada waktu Anda menandari user ID, pastikan ia ditandai oleh pemilik key! Hal yang sama juga berlaku jika Anda ingin menyediakan informasi tentang key Anda, termasuk key ID, fingerprint, dan ukuran key. ■

LEBIH LANJUT

- **http://www.cryptorights.org/pgp-help-team/hello.html**
- **http://www.mit.edu:8001/people/warlord/pgp-faq.html**
- **ftp://ds.internic.net/internet-drafts/draft-pgp-pgpformat-01.txt**
- **http://www.sni.net/~mpj/getpgp.htm**
- **http://web.cnam.fr/Network/Crypto/ (c'est en francais)**
- **http://www.freedomfighter.net/crypto/pgp-history.html**
- **http://www.paranoia.com/~vax/pgp_versions.html**
- **http://pgp.rivertown.net/**
- **http://www.stack.nl/~galactus/remailers/passphrase-faq.html**
- **http://www.stack.nl/~galactus/remailers/attack-faq.html**

Meskipun repot dan mahal, kadang beberapa konsumen menganggap perlu untuk menambah koneksinya. Namun, di antara koneksi yang ada mana yang lebih baik? USB, FireWire, atau SCSI?

Fadilla Mutiarawati



USB, FireWire, atau SCSI?

Pada saat akan membeli sebuah produk seperti printer, kamera, atau bahkan sebuah perangkat lain yang jauh lebih sederhana, kita kerap kali bertanya: "Koneksi apa yang digunakan? USB atau FireWire?" Atau tidak jarang juga timbul pertanyaan-pertanyaan: sebenarnya apa bedanya antara USB dan FireWire? Mengapa semua komponen tidak menggunakan koneksi yang sama saja? Bukankah dengan demikian konsumen tidak akan dibingungkan lagi.

Bahkan sekarang pilihan yang ada lebih bervariasi lagi. Karena setiap koneksi bisa memiliki lebih dari satu versi yang berbeda. Pada USB dan FireWire mungkin tidak terlalu riskan, karena keduanya hanya memiliki dua versi saja, Yaitu USB 1.1 dan USB 2.0 serta FireWire a dan FireWire B. Namun, lain halnya dengan SCSI yang memiliki lebih dari lima versi. Ada, SCSI Wide Ultra2 SCSI Ultra3 dan masih ada beberapa lagi. Selain versi, pin pun beragam. Beragamnya bentuk pin biasanya dipengaruhi, baik dari versi transmisi (misalnya pada SCSI) atau dapat juga dipengaruhi dari perangkat yang digunakan. Contohnya saja konektor USB pada kamera digital dengan konektor USB pada MP3 Player berbeda.

Untuk membeli produk tertentu, kita memang tidak dapat sembarang beli, melainkan kita harus mencocokkannya dengan apa yang sudah dimiliki oleh komputer. Meskipun tidak jarang juga seseorang akan dengan sengaja menambahkan koneksi baru agar mendapatkan transmisi yang lebih cepat.

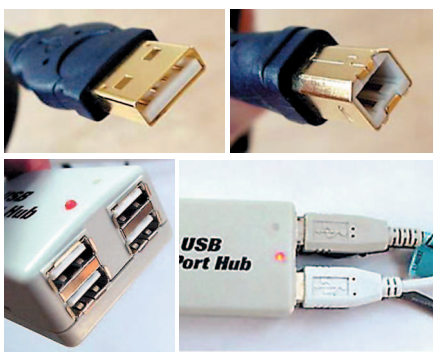
Salah satu yang menjadi pilihan selain USB dan FireWire adalah SCSI. Jika untuk komputer personal, kehadiran SCSI menjadi pilihan yang masih dapat ditawar. Lain halnya pada server atau komputer-komputer yang membutuhkan akses data yang cepat, maka kehadiran SCSI dianggap salah satu syarat.

Mana yang lebih baik USB, FireWire, atau SCSI? Pertanyaan yang benar bukan mana yang lebih baik, tapi mana yang paling tepat untuk kebutuhan Anda. Sebab setiap koneksi tidak hanya berbeda dalam hal biaya dan kecepatan saja. Ketiga koneksi yang disebutkan tadi juga memiliki karakter yang berbeda-beda satu sama lain. Oleh sebab itu, Anda harus jeli menelaah aplikasi yang akan digunakan sebelum memutuskan membelinya.

USB

Ketersediaan port USB sudah menjadi umum pada hampir seluruh komputer ataupun notebook keluaran tahun ini. Biasanya setiap komputer memiliki dua sampai empat port USB.

USB kali pertama dikembangkan untuk menggantikan port serial pada Mac dan port parallel pada PC. Meskipun kenyataannya, pada PC saat ini USB tidak hanya menggantikan port parallel saja melainkan juga serial. Lihat saja kini sudah banyak mouse, keyboard, gamepad, atau PDA yang biasanya menggunakan port serial kini juga menggunakan port USB.



USB; PIN, Port, dan Hub.

Awalnya USB yang diperkenalkan adalah USB 1.1, namun sekarang USB sudah berkembang menjadi USB 2.0. Walaupun kehadiran USB 2.0 sudah banyak melengkapi berbagai komputer dan notebook, bukan berarti USB 1.1 tidak lagi beredar. Saat ini, masih banyak beberapa produk atau komputer yang masih menggunakan USB 1.1.

Setiap sebuah kabel USB di dalamnya terdapat empat kawat kabel kecil. masing-masing berwarna merah, cokelat, kuning, dan biru. Merah untuk menghantarkan tegangan 5 Volt, cokelat untuk Ground, dan kuning-biru untuk mengirimkan data. Secara fisik bentuk konektor ada dua macam. Yang pertama disebut konektor A dan yang satu lagi disebut konektor B. Bila alat yang digunakan memiliki USB yang terpasang secara permanen, maka yang akan terhubung ke komputerlah dinamakan konektor A. Sedangkan bila alat menggunakan kabel terpisah, maka konektor yang terhubung pada alat dinamakan konektor B.

Pada USB, Anda lebih bebas memasang alat dibandingkan dengan serial atau parallel biasa. Sebab dengan USB, Anda dapat memasang alat dengan cara *plug n play* tanpa harus proses deteksi terlebih dahulu. Dan proses instalasi pun tidak dapat berjalan lebih mudah.

Kecepatan USB juga masih lebih baik dibandingkan dengan koneksi serial dan parallel. USB yang pertama (USB 1.1) memiliki kecepatan 1,5 MBps dan 12 MBps. Sedangkan USB dua memiliki kecapatan 20 kali lebih cepat dari USB 1.1, yaitu 480 MBps (sama dengan 60 MBps). Memang lebih cepat dari paralel biasa, namun tetap saja tidak lebih cepat dibandingkan FireWire b (100 MBps=800 MBps)) atau SCSI Ultra3 (160 MBps=1280 MBps).

Sekarang yang banyak beredar dipasaran adalah USB 2.0. Namun bukan berarti USB 1.1 ditinggalkan. USB ini masih tetap ada. Anda juga tidak perlu takut terhadap kompatibilitasnya bila menggunakan USB berbeda versi. Sebab keduanya tetap dapat berhubungan hanya saja kecepatannya akan mengikuti yang terendah.

Tidak hanya kecepatan yang menjadi kelebihan USB. Dengan sebuah konektor USB, Anda dapat menghubungkan 127 alat sekaligus. Yaitu dengan menggunakan alat yang dinamakan USB Hub. Biasanya satu USB Hub minimal memiliki empat koneksi. Namun salah satu yang menjadi kelemahannya adalah, hal ini akan membuat degradasi kecepatan pada koneksi.

Hub itu sendiri terbagi dua jenis, yang pertama adalah yang membutuhkan listrik sendiri atau yang disebut juga *powered hub*. Yang kedua adalah hub yang tidak menggunakan listrik atau disebut juga *unpowered hub*. Dalam memilih hub, yang perlu diperhatikan adalah alat yang akan dihubungkan. Bila alat tersbeut telah terhubung pada listrik seperti printer atau kamera yang menggunakan baterai, maka Anda dapat menggunakan unpowered hub. Tetapi apabila alat tersebut tidak terhubung pada listrik seperti mouse, harddisk eksternal, maka Anda dapat menggunakan powered hub. Sebab jarak yang terlalu jauh antara alat dengan komputer akan mengakibatkan alat tidak mendapatkan asupan listrik.

Dengan USB, jarak koneksi dapat lebih panjang dari parallel, yaitu dapat mencapai 30 meter dengan bantuan *repeater*. Bila tidak menggunakan repeater, maka setiap kabel mampu mengirim data sejauh 5 meter.

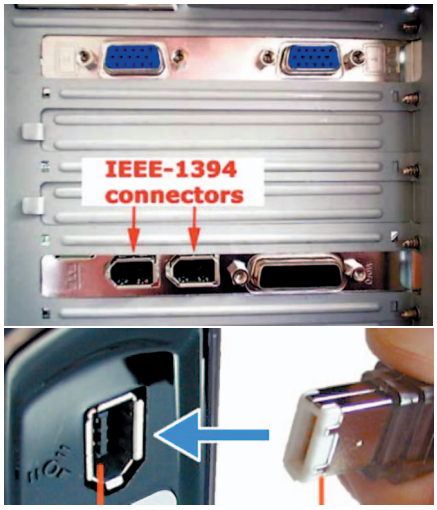
Jenis koneksi sebenarnya ada beberapa macam, yaitu *Interrupt*, *Bulk*, dan *Isochronous*.

Yang dimaksud dengan Interrupt adalah sejenis mouse atau keyboard. Data yang dikirimkan oleh peralatan ini sangat kecil dan datang di tengah-tengah aplikasi yang sedang berjalan.

Lain halnya dengan Bulk. Data yang dikirimkan oleh Bulk lebih besar dan tidak terkirim secara tiba-tiba atau ditengah aplikasi yang sedang berjalan. Salah satu contohnya adalah printer.

Sedangkan yang dimaksud dengan Isochronous adalah data yang terkirim secara terus menerus atau yang disebut juga *data streaming*. Salah satu contoh Isochronous adalah speaker.

Untuk keperluan dua hal yang pertama USB memang sangat tepat, namun untuk keperluan yang ketiga yaitu Isochronous agak sedikit sulit. Apalagi jika data tersebut termasuk jenis true isochronous, akan lebih sulit lagi.



Kabel dan port FireWire.

FireWire

Bila USB memiliki kelemahan dalam melakukan komunikasi data streaming atau Isochronous, tidak halnya dengan FireWire. FireWire kali pertama dikembangkan untuk memberikan kecepatan yang lebih baik dari USB.

FireWire yang pertama (FireWire a/ FireWire 400) memiliki kecepatan 400 MBps, jauh lebih besar dari USB 1.1, namun bukan berarti juga lebih lamban dari USB 2.0. Ada beberapa pengujian yang dilakukan antara USB 2.0 dengan FireWire a dalam memindahkan data dari sebuah harddisk, baik dengan tipe dan pada komputer yang sama. Pada pengujian tersebut diketahui bahwa FireWire a dapat membaca, sekaligus menulis lebih cepat dari USB 2.0. Ada dua situs yang dapat Anda kunjungi mengenai hal ini, yaitu *www.usb-ware.com/FireWire-vs-usb.htm* dan *www.barefeats.com/usb2.html*.

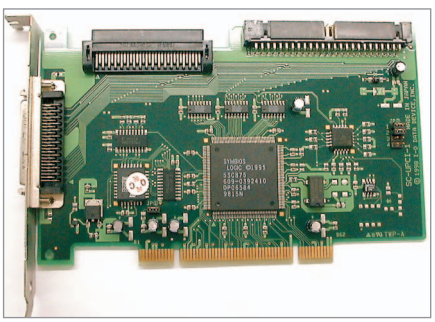
FireWire b atau disebut juga FireWire 800 memiliki kecepatan dua kali dari versi sebelumnya, yaitu 800 MBps atau sama dengan 100 MBps. FireWire ini jauh lebih cepat dibandingkan USB 2.0, namun masih lebih jauh jika dibandingkan SCSI Ultra3. FireWire 800 memiliki nilai kecepatan yang sama dengan SCSI Wide Ultra2.

Namun, ternyata tidak hanya kecepatan saja yang lebih unggul dari USB, FireWire dapat menangani transmisi data Isochronous dengan sangat baik. Oleh sebab itu, FireWire banyak digunakan untuk transmisi perangkat multimedia.

Meskipun kecepatan dan transmisi yang dimiliki oleh FireWire lebih baik, bukan berarti FireWire lebih unggul dari USB. Ada beberapa hal yang menjadi kelemahan FireWire. Misalnya saja jumlah perangkat yang dapat terhubung dengan FireWire tidak sebanyak USB. FireWire hanya memungkinkan 63 perangkat terhubung. Namun, setiap perangkat yang terhubung oleh sebuah FireWire dapat langsung digunakan oleh dua komputer/MAC sekaligus.

Berbeda dengan USB yang bersifat host base, FireWire bersifat *peer to peer*. Artinya, setiap peralatan dapat terhubung satu sama lain tanpa adanya bantuan dari komputer. Misalnya, dua buah kamera yang saling terhubung satu sama lain dnegan bantuan kabel FireWire. Hal ini berbeda dengan USB yang setiap alat harus terhubung pada komputer untuk dapat terkoneksi.

Dan kelemahan lain dari FireWire adalah diperlukannya alat tambahan berupa kartu FireWire untuk dapat menghubungkannya. Hal ini tentu saja menuntut dana yang lebih besar dibanding Anda menggunakan USB. Namun jika memang alat yang dimiliki membutuhkan kecepatan tinggi dan transmisi yang lebih konstan, maka FireWire patut menjadi opsi yang perlu dipertimbangkan.



Kartu SCS dan macam-macam pin SCSI.

SCSI

Jika Anda merasa USB dan FireWire masih kurang cepat, cobalah tengok SCSI (*small computer system interface*). SCSI adalah yang tercepat di antara ketiganya. Karena SCSI mampu mengeksekusi pekerjaan lebih efisien dibandingkan *interface* lain.

Seperti halnya FireWire, SCSI juga memerlukan kartu tambahan sebagai kontrol. Namun dari segi harga, SCSI jauh dibandingkan USB ataupun FireWire. Untuk sebuah kartu FireWire 400, Anda dapat membeli dengan harga kurang dari Rp300 ribu. Sedangkan harga sebuah kartu SCSI mulai dari Rp300 ribu lebih sampai jutaan rupiah.

Memilih SCSI juga tidak semudah memilih USB atau FireWire. SCSI ada berbagai jenisnya. Masing-masing jenis berbeda kecepatan maupun jumlah pin, sehingga dalam membelinya nanti diperlukan kehati-hatian.

SCSI merupakan perangkat *multi-threading*, kecepatannya tidak akan menurun seiring dengan jumlah *device* atau perangkat disambungkan kepadanya.

Kecepatan, fleksibilitas, dan biaya membuat SCSI tidak umum dipergunakan untuk kepentingan personal. Sebagian besar menggunakan SCSI untuk digunakan pada perangkat yang memang membutuhkan kecepatan dan kinerja yang andal. Contohnya seperti harddisk dan perangkat *back-up*. Dan biasanya yang menggunakan bukanlah komputer personal namun server. Tetapi sebagian perangkat grafis yang membutuhkan kecepatan dan *bandwidth* besar juga ada yang menggunakan SCSI sebagai interface-nya. Contohnya, scanner dan printer berukuran besar atau terkoneksi pada jaringan yang sibuk.

Sama dengan FireWire, SCSI kali pertama diperkenalkan oleh Apple sebagai interface tambahan pada MAC. Namun akhirnya, SCSI berkembang dan dapat dipergunakan pada semua *operating system*.

SCSI yang pertama dinamakan SCSI-1 dengan kecepatan 40 MBps dan jarak maksimal 6 meter, SCSI ini mampu menampung hanya delapan devices sekaligus. Kemudian versi keduanya SCSI-2 atau yang dikenal dengan "SCSI biasa" memiliki kecepatan yang dapat ditingkatkan sampai 80 MBps dan jumlah device pun dapat ditambahkan sampai dua kali lipat SCSI-1.

SCSI terus berkembang, sejak pertama diperkenalkan yaitu tahun 1981, kini SCSI sudah tersedia dalam sembilan varian. Yang tercepat adalah SCSI yang terakhir diluncurkan yaitu SCSI Ultra3, yang memiliki kecepatan 160 MBps (sama dengan 1280 MBps) dengan jarak tempuh maksimal 12 meter dan device yang terhubung 16 buah. Ultra3 juga dilengkapi dengan *Cyclical Redundancy Checking* (CRC) untuk memastikan integritas data yang ditransfer serta untuk validasi jaringan.

Dalam menggunakan SCSI, setiap device yang terhubung harus memiliki ID masing-masing. Pemberian ID ini dapat dilakukan dengan bantuan *software* tambahan khusus untuk mengontrol SCSI device yang digunakan. Setiap device yang terhubung akan dikurangi satu. Karena kartu SCSI itu sendiri akan ikut dihitung. Misalnya saja Ultra3 yang memiliki kemampuan menampung 16 device, maka pada kenyataannya ia hanya akan menampung 15 device saja. Sebab satu ID device-nya akan digunakan untuk kartu SCSI sebagai alat kontrol.

Jika dibandingkan FireWire jarak dan device yang dapat terhubung, SCSI tertinggal jauh. Namun, untuk kecepatan dan kestabilan masih lebih baik SCSI. Meskipun dari segi harga lebih mahal.

Mana yang akan dipilih? Sebaiknya lihat kembali apa yang akan dilakukan. Jika aplikasi Anda memiliki karakter Isochronous, maka gunakan FireWire. Atau bila hanya sekadar perangkat sederhana seperti mouse, keyboard, atau flash disk, gunakan saja USB. Namun bila perangkat tersebut adalah ruang back-up, terhubung ke jaringan yang sibuk, atau memang membutuhkan transmisi yang sangat stabil, sebaiknya Anda memilih SCSI. ■

LEBIH LANJUT

www.barefeats.com

Belum lama LCD digunakan pada proyektor, kini sudah ada LCOS. Namun, kehadiran LCOS dianggap belum mampu menggeser kebutuhan masyarakat terhadap proyektor DLP. Sebab biar bagaimanapun, antara DLP dan LCOS tetap berbeda.

Fadilla Mutiarawati

DLP, LCD, LCOS, Mana yang Lebih Baik?

Andi adalah seorang marketing eksekutif sebuah perusahaan komunikasi swasta. Pada sebuah presentasi, ia membawa sebuah tas yang sangat kecil yang ternyata berisi sebuah proyektor. Dan dalam melakukan presentasinya ia tidak lagi membawa komputer. Melainkan hanya dengan sebuah PDA yang terhubung menggunakan USB, presentasi pun berjalan dengan lancar.

Lain Andi lain pula halnya dengan Ryan. Untuk dapat memuaskan salah satu hobinya menonton film, Ryan membangun *home entertainment* di rumahnya dengan menggunakan proyektor. Menurutnya memasang sebuah proyektor lebih memuaskan dari pada hanya menggunakan televisi biasa. Selain ukuran, dari segi biaya ternyata proyektor lebih murah (untuk ukuran yang sama).

Meskipun keduanya menggunakan alat yang sama yaitu proyektor, namun proyektor keduanya memiliki beberapa perbedaan. Salah satu yang sangat terlihat adalah ukuran. Proyektor Ryan lebih besar ketimbang Andi. Sedangkan untuk perbedaan lain yang tidak terlihat masih banyak lagi. Mulai dari resolusi, cahaya, sampai teknologinya pun juga berbeda.

Perbedaan antara proyektor Andi yang banyak dipergunakan untuk presentasi bisnis dengan proyektor Ryan untuk home entertainment di rumahnya tidak menjadikan salah satunya menjadi lebih baik. Sebab biar bagaimanapun, di antara keduanya berada pada kelas yang berbeda.

Hal ini dapat menjadi catatan bahwa untuk membeli sebuah proyektor, maka tujuan akhir dari proyektor tersebutlah yang akan menentukan jenis/macam proyektor seperti apa yang akan dibeli. Tentu saja di samping *budget* yang dimiliki.

Berbicara tentang budget, sebenarnya apa saja yang menjadi parameter sebuah proyektor? Dan bagaimana memilih proyektor dengan tepat, sesuai kebutuhan.

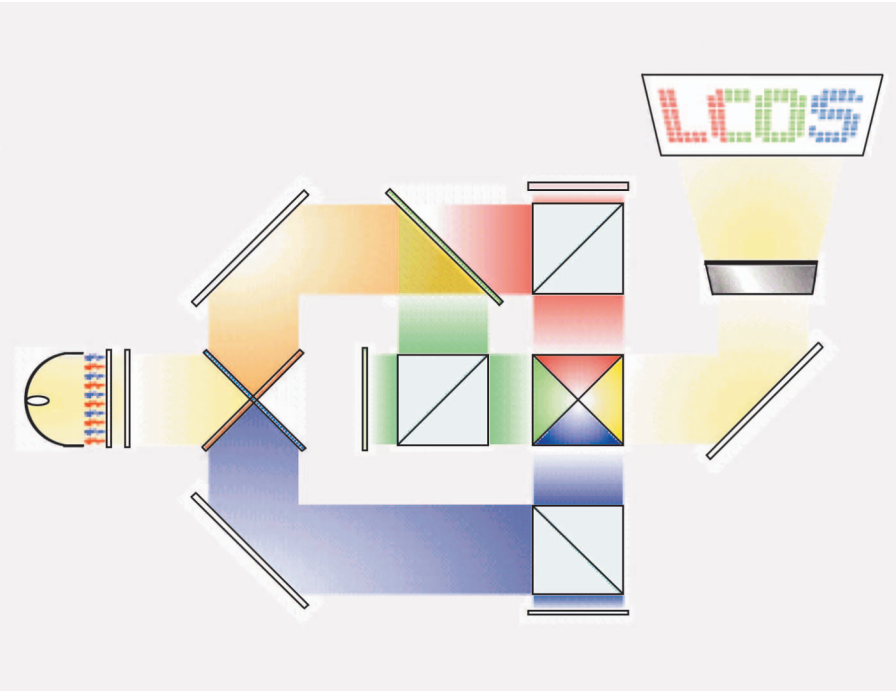
Teknologi

Salah satu yang dapat menjadi bahan pertimbangan pertama adalah teknologi yang digunakan. Setiap proyektor memiliki karakteristik berbeda-beda bila ditinjau dari teknologinya. Teknologi yang dimaksud di sini adalah teknologi pada *Image Engine* atau disebut juga *Light Engine*. Ada beberapa sistem Light Engine, yang banyak dikenal saat ini adalah CRT, DLP, LCD, dan yang terbaru adalah LCOS.

Light Engine adalah bagian yang memproyeksikan gambar. Dalam memproyeksikan gambar, Light Engine mendapatkan bahan berupa sinyal analog dari perangkat video decoder pada sebuah proyektor.

Dan bagaimana sebuah proyektor menampilkan gambarnya tersebut sudah membagi proyektor dalam dua jenis yang berbeda. Yang pertama adalah *Rear Projector* lalu yang kedua adalah *Front Projector*. Jika Rear Projector, berarti proyektor berada di belakang gambar sedangkan pada Front Projector sebaliknya yaitu proyektor berada di depan gambar.

Untuk Front Projector, mungkin sudah tidak asing lagi. Bentuknya sudah sangat umum, lain halnya dengan Rear Projector yang berbentuk seperti TV. Rear Projector sangat umum digunakan untuk di rumah. Selain karena bentuk fisiknya yang besar dan berat, kemampuan proyektor ini dalam mengakomodasi banyaknya penyimak sangat terbatas. Sebab proyektor dan layar telah di-



Sistem pada LCOS.

satukan dengan ukuran yang tidak mungkin di-*upgrade*.

Beda halnya dengan Front Projector. Pada Front Projector, proyektor dan layar tidak menyatu. Sehingga dapat diatur baik letak dan posisinya dengan lebih mudah. Selain itu, dalam mengakomodasi ruang dan penyimak yang lebih banyak Front Projector lebih leluasa. Tidak hanya layar yang dapat diperbesar, tapi juga proyektornya dapat diganti-ganti sesuai dengan kebutuhan.

Sistem yang dimiliki oleh Rear Projector dalam menampilkan gambar tidak berbeda jauh dengan Front Projector. Keduanya memiliki komponen dasar yang sama, yaitu Video Decode dan Light Engine. Namun dalam menampilkan gambarnya, Rear Projector menggunakan satu lensa tambahan yang berfungsi memantulkan sekaligus memperbesar gambar.

Teknologi Video Decode antara satu proyektor dengan lainnya hampir tidak memiliki perbedaan. Perbedaan yang signifikan memang banyak terjadi pada Light Engine.

● CRT

Proyektor yang menggunakan teknologi CRT berarti menggunakan tiga tabung CRT sekaligus dalam Light Engine-nya. Ketiga tabung ini memancarkan tiga sinar yang berbeda-beda, yaitu merah, hijau, dan biru. Adanya tiga tabung yang berbeda-beda warna dalam proyektor CRT, membuat proyektor ini lumayan besar dan berat. Sehingga dianggap kurang fleksibel untuk digunakan pada presentasi-presentasi dalam ruang yang kecil.

● DLP

Digital Light Processing atau yang disingkat dengan DLP kali pertama dikembangkan oleh Texas Instrument. Pada DLP, cahaya terlebih dahulu akan mengenai sebuah *Color Filter* berbentuk roda. Kemudian warna yang diperoleh akan mengenai *Digital Micromirror Devices* (DMD). Dari DMD inilah kemudian cahaya akan diproyeksikan dengan cara dipantulkan ke layar.

DMD adalah sebuah optical chip yang terdiri dari tiga lapis cermin-cermin micro yang masing-masing lapisan dipisahkan oleh rongga udara yang memungkinkan cermin untuk miring sejauh -10 sampai +10 derajat. Kemiringan setiap cermin DMD akan diatur oleh sebuah chip khusus yang ada pada DMD.

Keberadaan DMD membuat DLP hanya membutuhkan satu set optic saja. Kesederhanaan ini membuat proyektor DLP lebih ringkas dan ringan. Beratnya dapat mencapai kurang dari 250 gram.

Contrast Ratio dan struktur pixel DLP juga lebih baik. Hal ini disebabkan oleh sistem *transmisive* yang dimiliki oleh DLP. Meskipun pada beberapa sisi DLP lebih baik dari LCD, DLP juga memiliki kekurangan. Penggunaan *colorwheel* pada DLP mengurangi nilai *brightness* proyektor. Dari segi harga, proyektor DLP juga lebih mahal, sebab ongkos produksi yang dibutuhkannya memang tinggi.

● LCD

Jika DLP disebut juga dengan teknologi *reflective* karena menggunakan sistem pantulan. Sedangkan LCD disebut juga teknologi transmisive, yakni meneruskan cahaya. Sebab cahaya yang masuk pada LCD setelah melalui proses penyaringan menggunakan cermin Dichroic akan diteruskan secara langsung ke layar proyektor.

Cermin Dichroic atau disebut juga Dichroic Mirror memisahkan warna menurut gelombangnya. Ada tiga warna dasar yang dihasilkan oleh cermin tersebut yaitu merah, biru, dan hijau. Ketiga warna ini dihasilkan dengan tiga cermin yang masing-masing menyaring warna berbeda.

Teknologi LCD sudah dianggap cukup stabil dan biaya panelnya pun cukup rendah, sehingga memungkinkan menggunakan tiga panel LCD (RGB) sekaligus dalam satu proyektor. Hal ini membuat gambar yang dihasilkan proyektor memiliki warna yang cukup bagus. Begitu pula halnya dengan cahaya yang sudah sangat baik. Sayangnya, sistem transmisive telah membuat timbulnya artefak pada gambar sehingga membuat gambar seperti terkotak-kotak. Dan dikarenakan pada proyektor LCD polarisasi gambar tidak terjadi 100%, maka *contrast ratio* LCD lebih rendah dari DLP. Di samping itu, daya tahan LCD terhadap panas juga tidak mampu terlalu lama. Berbeda dengan DLP yang dapat bertahan sangat lama.

● LCOS

Teknologi yang terakhir ini memanfaatkan keunggulan dua teknologi yang sudah hadir sebelumnya, yaitu LCD dan DLP. Teknologi LCOS lebih mudah dipro-

duksi dan ringan dibandingkan LCD. Resolusi yang dihasilkan juga lebih baik dari LCD.

Bahkan resolusi teknologi ini diperhitungkan dapat mencapai QXGA, yaitu 2048x1536 pixel. Sangat tinggi, bahkan yang tertinggi. Teknologi ini juga mengurangi artefak yang muncul pada LCD. Selain itu, LCOS memiliki kontrol analog seperti layaknya LCD dengan gradasi warna yang lebih baik dibandingkan DLP. Contrast ratio teknologi ini juga lebih baik dibandingkan LCD meskipun tidak terlalu lebih baik dari DLP. Namun, nilai brightness-nya sejajar dengan LCD yang artinya lebih baik dari DLP.

Resolusi

Parameter lain yang juga perlu diperhatikan adalah resolusi. Semakin baik resolusi memang akan menghasilkan gambar yang semakin baik juga. Namun berkaitan dengan resolusi, tidak semua aplikasi membutuhkan resolusi yang tinggi. Ada baiknya jika pemilihan resolusi disesuaikan dengan kebutuhan. Sebab biar bagaimanapun, semakin tinggi resolusi sebuah proyektor, harga proyektor tersebut pun akan semakin mahal.

Biasanya, resolusi pada proyektor diwakilkan dengan sebutan-sebutan seperti SVGA, XGA, SXGA, dan UXGA.

- **SVGA**

Yang dimaksud dengan SVGA adalah proyektor memiliki resolusi 800x600 pixel. Resolusi ini sangat cocok untuk digunakan keperluan presentasi sederhana. Yang dimaksud dengan presentasi sederhana adalah presentasi-presentasi yang tidak menampakkan gambar-gambar yang kompleks hanya seputar teks, grafik, dan diagram biasa saja.

- **XGA**

Nilai resolusi pada proyektor XGA adalah 1024x768 pixel. Gambar yang dihasilkan oleh proyektor XGA lebih jernih dibandingkan proyektor dengan resolusi SVGA, sehingga penggunaannya dapat lebih luas. Projector XGA dapat digunakan untuk melakukan presentasi yang lebih banyak menggunakan warna dibanding presentasi dengan SVGA.

- **SXGA**

Bila ada presentasi yang sangat kompleks, banyak menampilkan tidak hanya grafik dan diagram saja, melainkan gambar-gambar desain seperti gambar teknik atau iklan, maka sebaiknya presenter menggunakan proyektor dengan resolusi SXGA.

Proyektor dikatakan memiliki resolusi SXGA berarti proyektor tersebut memiliki resolusi sebesar 1280x1024 pixel. Proyektor dengan resolusi tinggi ini juga cocok untuk digunakan sebagai layar pada home entertainment Anda. Karena untuk menonton sebuah film memang dibutuhkan resolusi yang tinggi. Lagipula harga sebuah TV projector lebih murah dibandingkan TV biasa dengan ukuran yang sama. Oleh sebab itu, tidak ada salahnya bila Anda menggunakan proyektor ini untuk di rumah sebagai pengganti TV.

- **UXGA**

Proyektor dengan resolusi UXGA sampai saat ini masih sangat mahal dan jarang. Proyektor beresolusi 1600x1200 pixel ini lebih cocok digunakan oleh para profesional yang bergerak di bidang *imaging* untuk melakukan presentasi. Atau bagi Anda yang memang memiliki dana berlebih untuk home entertaiment.

- **QXGA**

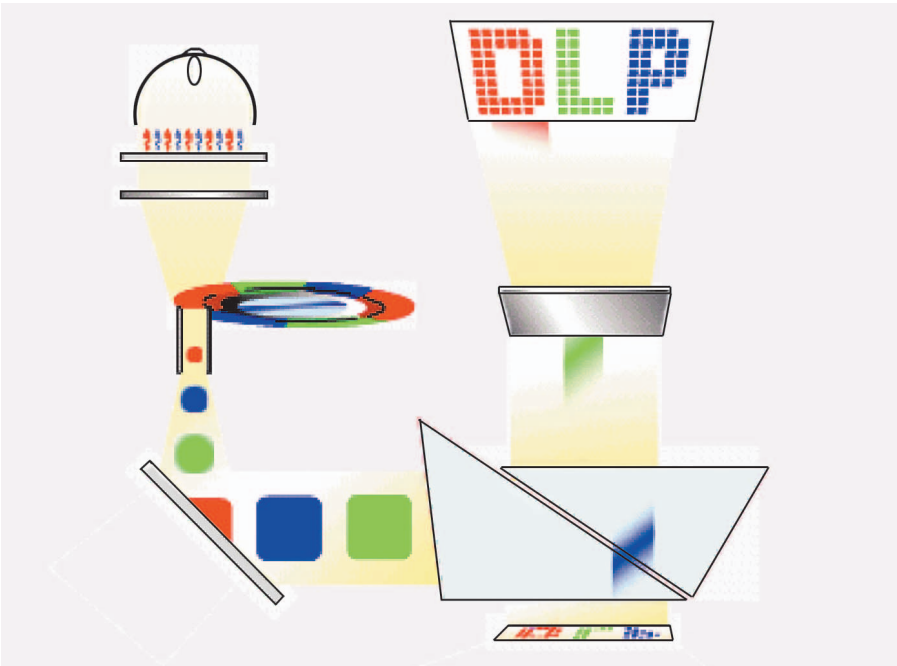
Sampai saat ini, proyektor yang memiliki resolusi QXGA masih sangat jarang. Salah satunya adalah proyektor yang diproduksi oleh JVC. Proyektor tersebut menggunakan sistem LCOS dengan sebuah chip yang dinamakan D-ILA. Yang dimaksud dengan resolusi QXGA adalah proyektor beresolusi 2048x1536 pixel. Hampir tujuh kali lebih besar dari SVGA.

Brightness

Setelah resolusi, hal lain yang dapat ikut diperhitungkan adalah nilai *brightness*. Nilai brightness diwakilkan oleh satuan ANSI (American National Standar Institute), yaitu Lumens. Semakin besar nilai ANSI Lumens-nya, maka akan semakin terang proyektor tersebut. Dan semakin terang sebuah proyektor, maka nilainya juga akan semakin baik. Hanya saja nilai brightness juga akan mempengaruhi harga. Semakin terang, semakin mahal proyektor tersebut.

Brightness ini akan sangat berguna bila ternyata presentasi dilakukan di tempat yang tidak terlalu gelap. Sebab pada tempat yang terang, tandanya Anda membutuhkan cahaya proyektor yang lebih terang lagi.

Jangan lupa juga untuk memeriksa daya tahan lampu. Lampu proyektor tergolong mahal, tidak ada salahnya jika Anda memperkirakannya juga.

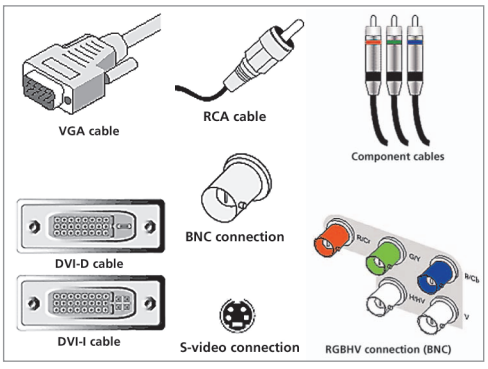


Sistem pada DLP.

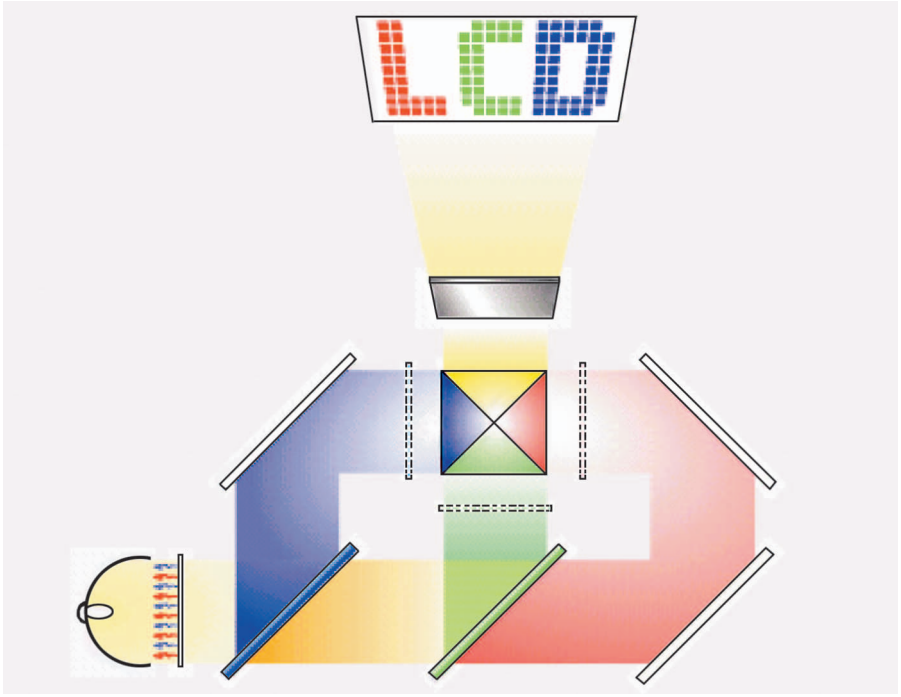
Koneksi

Aspek lain yang tidak boleh luput adalah koneksi pada proyektor yang Anda beli. Ketersediaan koneksi harus disesuaikan dengan kebutuhan. Agar apa yang akan Anda lakukan dengan proyektor tersebut tercapai. Koneksi ini juga dapat mempengaruhi kualitas gambar yang Anda lihat. Berikut adalah koneksi yang dapat Anda periksa:

- VGA: ini adalah koneksi video yang akan menghubungkan proyektor dengan komputer, baik PC maupun notebook. Koneksi ini sangat wajib tersedia pada proyektor yang memang digunakan untuk presentasi melalui komputer.
- RGB Cable: Bentuknya menyerupai BNC, namun warna masing-masing jack adalah RGB dan putih. Koneksi RGB biasanya untuk dikoneksikan ke komputer yang tidak menggunakan koneksi VGA. RGB kabel ada tiga macam. Yang pertama RGBHV yang memiliki lima jack, yaitu merah, hijau, biru, horizontal, dan vertikal.
- Ada juga RGBH/V dengan 4 jack, sinyal horizontalnya digabungkan dengan vertikal. Dan yang terakhir adalah 3 jack, RGB Sync on Green yang artinya sinyal sinkronusnya tidak terpisah secara horizontal/vertikal melainkan digabungkan dan dibawa oleh jack yang hijau.
- RCA: Kabel RCA adalah kabel yang sudah sangat umum digunakan hampir pada semua perangkat home entertainment di rumah. Mulai dari CD/DVD player, VCR, camcorder, juga televisi. RCA ada tiga warna yang umumnya adalah merah, putih, dan kuning. Merah dan putih untuk audio dan kuning untuk video.



Berbagai macam koneksi.



Sistem pada LCD.

- BNC: Antara BNC dengan RCA hanya berbeda secara fisik, keduanya memiliki fungsi yang sama yaitu membawa sinyal audio dan video dengan tiga macam sekaligus. BNC memiliki bentuk yang lebih aman. Bila Anda membeli proyektor dengan BNC, tetapi di rumah masih banyak yang menggunakan RCA, maka Anda dapat mencoloknya terlebih dahulu ke sebuah adapter.
- S-Video atau Y/C: Jika pada RCA atau BNC sinyal video hanya ditransmisikan dengan stau koneksi saja, maka dengan S-Video akan terbagi dua, yaitu *luminance* dan *chrominance*. Sinyal yang dihantarkan pun jadi lebih baik ketimbang RCA atau BNC. Biasanya koneksi ini ada pada produk-produk kelas atas.
- Component: koneksi ini selangkah lebih maju lagi dari S-Video. Karena dibandingkan hanya dua, Component membagi sinyal Video menjadi tiga yaitu Y, Cr, Cb atau Y, Pb, Pr. Namun untuk pemakai komputer, mungkin agak membingungkan sebab masing-masing kabel akan ditandai dengan warna-warna RGB (Merah, Hijau, Biru). Meskipun demikian, bila pada komputer bentuk jack-nya seperti BNC, sebaliknya Component bentuk jack-nya seperti RCA. Component biasanya tersedia pada DVD player *High End* atau pada tuner HDTV.
- DVI: Koneksi ini belum banyak tersedia di pasaran mengingat DVI belum memiliki standar yang umum. Sehingga setiap produsen memiliki standarnya sendiri-sendiri.

Ukuran

Ukuran juga ikut mempengaruhi pilihan. Bila Anda termasuk seorang pebisnis yang banyak melakukan presentasi di mana-mana, maka ukuran yang mungil dapat menjadi pilihan. Meskipun harganya memang lebih mahal, ketimbang yang agak besar. Namun bagi Anda yang ingin memiliki Front Projector di rumah, Anda dapat mengenyampingkan ukuran sebab ukuran menjadi parameter yang kedua setelah resolusi.

Mana pilihan Anda? Tidak perlu memilih yang terbaik dari parameter yang ada, yang penting proyektor yang Anda beli sesuai dengan yang dibutuhkan. Lagi pula yang terbaik adalah yang tepat dengan kebutuhan Anda dan bukan yang termahal. ■

LEBIH LANJUT

www.projectisle.com.au

Desktop Search berbeda dengan fitur search yang ada pada Windows yang Anda gunakan. Namun jika tidak hati-hati menggunakan Desktop Search, data Anda dapat saja jatuh pada tangan yang tidak bertanggung jawab.

Fadilla Mutiarawati

Desktop Search, Search Engine Pribadi

Beberapa hari yang lalu, penulis harus membeli sebuah harddsik baru dengan kapasitas 80 GB. Hal ini penulis lakukan karena dengan harddisk yang lama berukuran 40 GB, data baru sudah tidak memiliki ruang lagi. Jika dijumlahkan, maka penulis memiliki ruang data hampir sebesar 150 GB ditambah dengan data pada media *back-up* yang belum disebutkan.

Apa saja data yang penulis simpan? Selain data pekerjaan, penulis juga menyimpan banyak sekali data video dan *image*, baik hasil jepretan kamera sendiri, dari Internet, atau hasil olahan. Selain itu, penulis juga menyimpan data lainnya yang tidak kalah besar. Seperti kumpulan lagu, artikel, atau buku digital yang penulis peroleh baik dari Internet maupun dari tempat lain.

Data pekerjaan juga bukanlah data sederhana, di dalamnya terdapat berbagai macam format file mulai dari file dokumen sampai file multimedia, seperti gambar, audio, sampai video.

Belum lagi data dari MS Outlook yang semakin hari juga semakin menumpuk. Seperti e-mail dan *address book*. Saya tidak pernah merasakan kerugian yang sangat berarti mengenai ruang simpan ini, mengingat semua data tersimpan dengan sistem pemetaan yang cukup baik dan rapi. Namun, ketika penulis hendak mencari beberapa lintas aplikasi seperti data dalam Outlook maupun data dalam harddisk dan file-file *attachment*, barulah penulis menyadari betapa menyebalkannya. Sebab selain waktu yang relatif lama, penulis juga harus melakukan pencarian dengan aplikasi yang berbeda-beda. Misalnya untuk mencari data pada MS Outlook, harus melakukannya dalam MS Outlook tersebut, begitu pula halnya dengan file-file pdf harus menjalankan terlebih dahulu Acrobat Reader-nya. Memang sangat merepotkan, tetapi hal ini tidak berlangsung lama, sebab tidak berselang lama saya menginstal aplikasi yang dinamakan Desktop Search.

Belakangan, aplikasi Desktop Search mulai sering dibicarakan. Hal ini berkaitan dengan peluncuran Desktop Search yang dilakukan oleh tiga perusahaan *search engine* terbesar, yaitu Yahoo!, Google, dan MSN. Padahal sebenarnya, aplikasi Desktop Search tidak hanya dikembangkan oleh mereka saja, masih ada beberapa perusahaan search engine lain yang berinisiatif membuatnya, contohnya seperti Ask Jeeves dan HotBot.

Sebenarnya apa yang dimaksud dengan Desktop Search dan apa manfaatnya? Mengapa keberadaannya perlahan-lahan menjadi kebutuhan yang sangat diperhitungkan selain operating system-nya.

Windows Search [1] Desktop Search

Setiap kali menginstal Windows, maka Anda akan mendapatkan sebuah fitur yang dinamakan *Search* untuk melakukan pencarian data pada komputer Anda. Namun, apa yang Anda miliki tersebut lebih tepat dikatakan Windows

Search dibandingkan dengan Desktop Search. Mengapa demikian?

Sebelum menjawab pertanyaan tersebut, ada baiknya mengetahui terlebih dahulu apa yang dimaksud dengan Desktop Search. Desktop Search adalah *searching tool* yang berintegrasi dengan hampir seluruh aplikasi di dalam sebuah komputer. Artinya, Anda tidak perlu lagi mencari data pada file dari aplikasi tertentu dengan membuka aplikasinya terlebih dahulu. Contohnya file MS Outlook, Website, ataupun PDF.

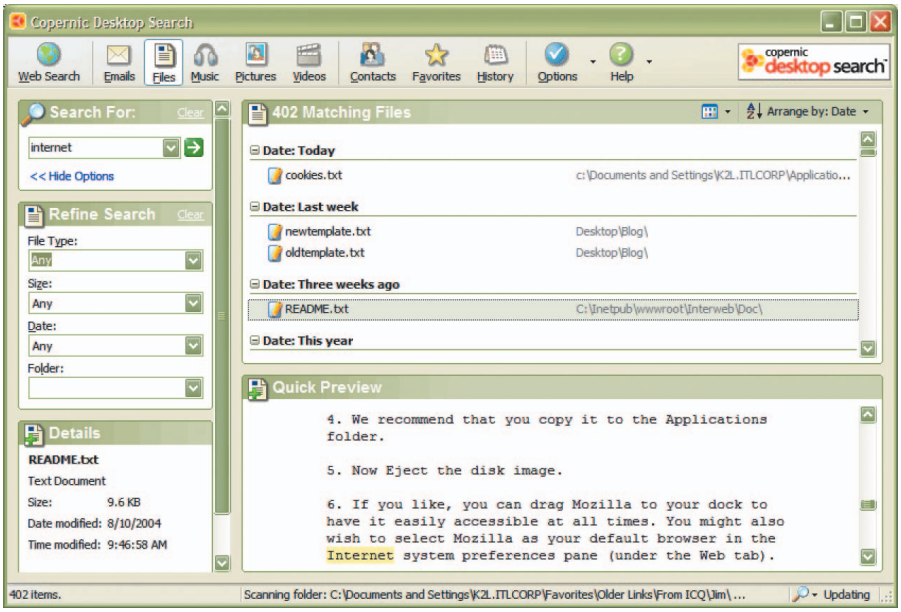
Salah satu yang menjadi ciri khas Desktop Search adalah penggunaan Database. Database ini merupakan indeks dari data yang ada dalam komputer. Sehingga pada saat mencari komputer akan melakukan pencarian ke dalam database yang sudah terbuat. Hal ini berbeda dengan Windows Search yang ada sekarang, yang memeriksa secara satu per satu file untuk mencari yang dimaksudkan. Ketidakberadaan database pada Windows Search menjadikannya berjalan cukup lama. Apalagi jika ruang yang diperiksa termasuk luas dan penuh.

Selain ketidakberadaan database, Windows Search juga tidak memiliki integrasi dengan aplikasi lain. Misalnya saja bagi yang ingin memeriksa file PDF yang memuat kata "Decideous", Anda harus membuka aplikasi Acrobat Reader terlebih dahulu dan baru dapat mencarinya.

Integrasinya bahkan tidak hanya berkaitan dengan format file aja, namun ada juga Desktop Search yang memiliki integrasi dengan lokasi harddisk. Contohnya, Desktop Search milik Google yang juga dapat digunakan untuk melakukan pencarian pada harddisk dalam Intranet. Misalnya saja folder *My Document* yang Anda miliki ternyata sumbernya berada pada harddisk di server. Maka, Google akan mengindeks juga data dalam harddisk tersebut dan Anda dapat mencari file di dalamnya.

Proses Indexing

Dalam membuat database, Desktop Search melakukan peng-*index*-an terhadap file-file yang ada pada lokasi yang diinginkan. Proses peng-index-an yang utama berjalan pada saat setelah proses instalasi dilakukan. Proses yang pertama ini memang lebih memakan waktu. Dan semakin banyak data yang Anda miliki, maka semakin lama juga proses indexing berlangsung.



Tampilan interface Copernic.

Setelah proses indexing yang kali pertama selesai, maka aplikasi Desktop Search sudah dapat Anda gunakan. Tetapi, bukan berarti proses indexing telah berhenti bekerja. Proses tersebut akan terus berlangsung selama data pada komputer Anda bertambah.

Perlu ketelitian tertentu pada saat akan menginstal Desktop Search, yaitu bagaimana proses indexing berlangsung setelah yang kali pertama dilakukan. Ada Desktop Search yang melakukan proses indexing pada *background system* yang sedang berjalan. Dan ada juga Desktop Search yang melakukan proses indexing pada saat system dalam keadaan *idle*. Jika proses indexing berjalan pada komputer sibuk, hal ini tentu saja akan memakan *resource* komputer, baik processor maupun RAM.

Hasil dari index sendiri yaitu database-nya, juga akan memakan resource harddisk Anda. Sebanyak apa tergantung pada aplikasi Desktop Search tersebut serta banyak dan kompleksnya data Anda.

Longhorn

Jika saat ini Windows Search tidak sama dengan Desktop Search, maka lain halnya dengan nanti. Tepatnya pada saat Windows Longhorn diluncurkan. Sebab salah satu pengembangan yang dilakukan oleh Microsoft terhadap Windows versi barunya adalah system file yang jauh lebih baik. System file tersebut dinamakan WinFS. Dengan WinFS, maka data dalam komputer akan di-index dan hasilnya disimpan ke dalam database khusus. Sehingga pada saat user mencari file tertentu, ia akan mendapatkan hasilnya dalam waktu yang sangat cepat.

Kecepatan bukan semata-mata efek dari WinFS, tetapi integrasi antaraplikasi juga menjadi bagian di dalamnya. Bila Anda mencari file yang memuat sebuah nama, maka yang akan muncul sebagai *result*, tidak hanya file dokumen yang memuat nama tersebut. Namun, Anda juga dapat melihat file Outlook (Address Book, e-mail, dan lain-lain) yang memuat nama tersebut sebagai hasilnya.

Pada WinFS, tidak hanya isi dari file saja yang akan di-index, melainkan metadata sebuah file juga akan ikut serta ter-index. Sehingga nantinya Anda juga dapat mencari file dengan menggunakan bagian dari metadata sebagai petunjuknya. Misalnya, mencari file dengan menggunakan nama pembuat file sebagai petunjuk.

Longhorn memang sangat canggih, namun jika hanya untuk fitur search-nya saja sebenarnya Anda tidak perlu me-

nunggu Longhorn yang masih sangat lama. Sebagai pengganti, saat ini Anda dapat saja menginstal Desktop Search lain yang tidak kalah andalnya.

Masih Versi Beta

Keberadaan desktop sudah banyak dinanti-nanti. Dan hal ini disadari penuh oleh perusahaan search engine. Oleh sebab itu, mereka membangun sistem search engine-nya ke dalam bentuk mini. Agar dapat digunakan pada komputer-komputer pribadi. Sebagian besar memang baru versi beta. Seperti MSN Desktop Search, Yahoo! Desktop Search, Google Desktop Search, Ask Jeeves, dan Copernic. Masing-masing memiliki tidak sama baik dari segi kemampuan maupun data yang dihasilkan.

MSN

MSN Desktop Search yang menggunakan interface yang sangat bersahabat tidak melakukan proses indexing terhadap *history* web-nya, serta hanya dapat dijalankan dengan IE. Meskipun Desktop Search ini juga menangani metadata.

Yahoo!

Jika yang lain tidak memeriksa file *attachment* atau hanya sekadar melakukan *scanning* pada nama file-nya saja, sebaliknya Yahoo! melakukan scanning pada isi attachment. Search Desktop dari Yahoo! Juga men-*support* format file yang sangat banyak.

Google

Google yang menggunakan interface sama dengan web-nya, menawarkan fitur mencari lewat jaringan. Ini sangat menarik, namun sebagian user banyak juga yang masih meragukan tingkat keamanan dan privacy-nya.

Ask Jeeves

Salah satu yang sangat cepat dalam melakukan proses indexing adalah Ask Jeeves. Namun sayangnya, Ask Jeeves memiliki *support* format yang terbatas.

Copernic

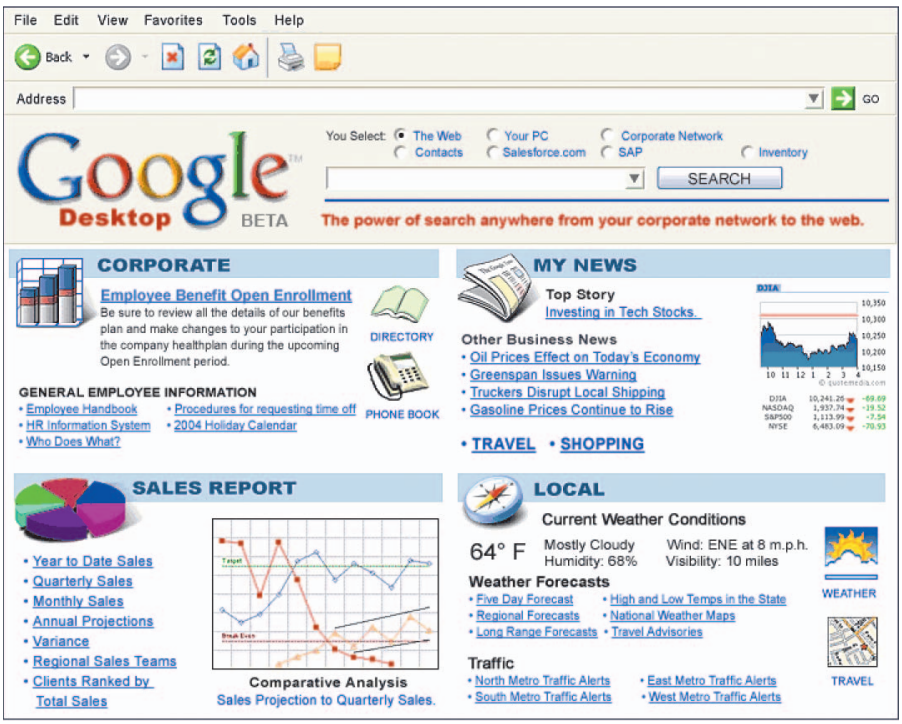
Yang terakhir ini memang bukan pemain kelas atas, namun aplikasi Search Engine-nya patut diperhitungkan. Interface Copernic cukup baik, meskipun sedikit kaku. Namun, Copernic dapat menangani berbagai macam format file.

Memilih Dekstop Search

Dalam memilih sebuah Desktop Search, ada beberapa hal yang memang perlu dipertimbangkan jika Anda memiliki berbagai macam pilihan. Meskipun semua search engine tersebut kini dapat Anda peroleh secara cuma-cuma. Tetap saja akan menjadi membebankan jika Anda harus menginstal semuanya. Bukan saja memakan ruang, tetapi juga kerja komputer dapat semakin lamban.

Apa saja yang perlu diperhatikan:

- Proses Indexing. Ini adalah salah satu proses utama, sebab pada saat file dicari, database inilah yang akan digunakan. Seberapa jauh proses indexing membebankan komputer perlu diperhatikan, terutama bagi komputer yang memiliki resource terbatas? Misalnya saja Desktop Search yang menjalankan proses indexing pada saat komputer bekerja, tetapi ada juga yang menjalankan proses indexing pada saat komputer berada dalam keadaan *idle*.
- Dukungan File. Semakin banyak format file yang dapat di-index dan dicari, maka semakin baik Desktop Search tersebut. Ada beberapa Desktop Search yang mampu mencari ke dalam format PDF, tetapi ada juga yang harus menggunakan *plug-in* tambahan atau bahkan sama sekali tidak mampu.
- Interface. Bagaimana interaksi aplikasi dengan Anda juga dapat dipikirkan. Semakin mudah cara mengoperasikannya juga akan semakin membantu. Misalnya saja menggunakan interface yang sama seperti layaknya Windows search atau Internet search engine yang sudah dikenal secara umum.
- Privacy juga dapat ikut dipertimbangkan, khususnya bagi Desktop Search yang dapat dilakukan dalam jaringan. Anda harus benar-benar pelajari mekanismenya jangan sampai malah merugikan. Masalah privacy sampai saat ini menjadi salah satu yang cukup ramai diperdebatkan berkaitan dengan Desktop Search. ■



Tampilan *interface* Google Desktop Search.

LEBIH LANJUT

- **desktop.google.com**
- **desktop.yahoo.com**
- **www.copernic.com**
- **sp.ask.com/docs/desktop**

Start merupakan operasi paling fundamental yang dilakukan Windows, tetapi apakah Anda tahu apa yang terjadi di belakang pada waktu program dijalankan?

Gunung Sarjono

Jalankan Saya!

Coba pikirkan pertanyaan berikut. Apakah PC Anda berjalan lambat atau kekurangan RAM? Apakah Anda melihat banyak aktivitas disk pada waktu tidak ada orang yang menggunakan sistem? Pernahkan mengira bahwa Anda telah terkena virus? Untuk menjawab pertanyaan tersebut, Anda perlu mengetahui apa yang berjalan pada PC Anda, tetapi itu tidaklah mudah.

Anda mungkin mulai dengan melihat icon-icon pada *Taskbar*, misalnya, tetapi mereka tidak bisa berkata banyak. Aplikasi bisa memilih untuk tidak dimasukkan ke situ. Memanggil *Task Manager*? Itu lebih baik, tetapi masih membingungkan. *Tab Application*, misalnya, tidak benar-benar menampilkan aplikasi. *Tab Processes* membawa Anda lebih dekat terhadap kebenaran, tetapi program yang Anda lihat di situ juga tidak "benar-benar berjalan." Untuk memahami semuanya, kita perlu melihat dari awal sekali: apa yang terjadi pada waktu Anda mengklik ganda file *executable*?

Arti "Run" Sebenarnya

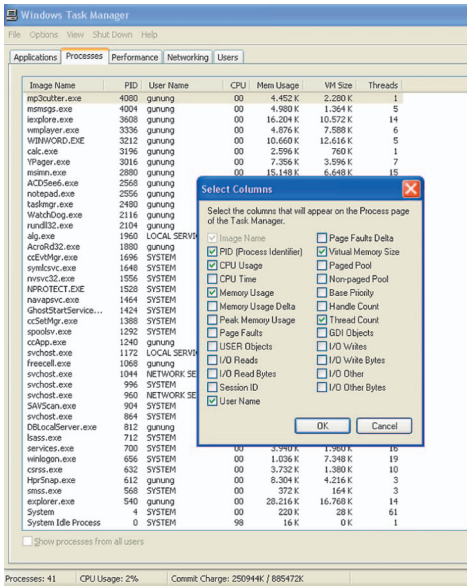
Mudah untuk dilupakan, tetapi Windows sebenarnya mendukung beberapa jenis file *executable*. Setelah Anda mengklik ganda pada sesuatu, yang menjadi tantangan adalah mencari tahu jenis file tersebut.

Untuk mengetahuinya, Windows membuka dan membaca beberapa *byte* pertama. Dalam istilah progamming disebut "Header", yang berisi info lebih banyak tentang file. Sebagai contoh, file EXE dapat dikenali dari dua karakter pertama yang selalu MZ. Setelah jenis file dikenali, Windows memilih siapa yang menjalankannya. Program 32-bit ditangani oleh kernel; DOS atau software 16-bit (Windows 3.1) dijalankan oleh komponen Windows bernama NTVDM.EXE (NT Virtual DOS Machine); file *batch* (.bat atau .cmd) dikirim ke CMD.EXE.

Memeriksa bagian dalam file bisa menimbulkan masalah keamanan yang cukup riskan, jadi ini berarti Anda tidak dapat mengandalkan *extension* file. Sebagai contoh, "Trojan.exe" bisa diganti namanya sebagai "Harmless.bat"; Anda mungkin menganggapnya sebagai file batch biasa, tetapi pada waktu mengklik-ganda akan menjalankan program sebagai executable. Seperti biasa, jangan percaya siapapun dan apapun.

Program yang Menyamar

Setelah Windows mengetahui ia bekerja dengan program Windows 32-bit, ia siap untuk mulai menjalankannya. Namun bagaimana? Microsoft mempunyai metode "back door" di mana dengannya aplikasi dapat dijalankan dengan beragam cara, misalnya menggunakan proses pengaturan memory yang lebih



Pilih informasi yang ingin ditampilkan pada *Task Manager*.

JALANKAN DI SINI

■ Sekilas tab *Process* pada *Task Manager* akan memberitahukan bahwa banyak *software* yang sedang berjalan pada PC Anda. Beberapa di antaranya mungkin menginstalasi dirinya sendiri supaya di-*load* pada waktu Windows berjalan, tanpa lebih dulu bertanya kepada Anda. Terganggu? Mempelajari di mana startup tersebut berada bisa jadi membantu dalam mengidentifikasi dan menghilangkan mereka.

Folder Startup sudah pasti menjadi calon, itulah sebabnya kebanyakan progam bersembunyi di tempat lain. Jalankan Registry Editor, buka HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion, dan cari key seperti Run, RunOnce, RunOnceEx dan RunServices. Anda akan menemukan beragam program startup, tetapi ingat bahwa Anda mungkin mempunyai key yang sama pada HKEY_CURRENT_USER. Beberapa software dijalankan melalui file Win.ini. Buka file tersebut dan cari baris run= dan load. Yang lainnya dijalankan dari file System.ini. Cari baris shell= yang menunjuk ke Explorer.exe (shell=Explorer.exe), tanpa nama tambahan (shell=Explorer.exe Trojan.exe).

Cara yang sama juga kadang-kadang digunakan pada registry, di mana program menambahkan path dan nama file-nya sesudah "Explorer.exe". Dan itu terus berlanjut, dengan banyak pilihan tempat bagi kode untuk bersembunyi. Tidak bisa mengingat mereka semua? Jangan khawatir karena itu tidak perlu. DiamondCS Autostart Viewer merupakan tool gratis yang menampilkan semua program yang berjalan otomatis, dan memungkinkan Anda untuk mengubah atau menghapus mereka sesuka hati.

sederhana, atau me-*load debuggger* pada waktu aplikasi dijalankan.

Pada situasi biasa Anda tidak tahu tentang ini, kecuali karena ini juga memberikan peluang bagi Trojan untuk mengacau. Berikut adalah bagaimana Anda menggunakannya untuk bersenang-senang dengan anggota keluarga yang lain atau teman. Jalankan Registry Editor, dan buka key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Extension Options. Buatlah subkey bernama iexplore.exe. Klik key Anda yang baru, dan dari menu Edit, pilih New, dan kemudian klik String Value. Beri nama Debugger. Klik ganda string dan ketik calc.exe. Tutup semua jendela Internet Explorer, kemudian restart browser. Anda akan melihat Calculator. Menyenangkan, bukan? Sekarang hapus key registry yang baru saja Anda buat (pastikan Anda tidak mengapa-apakan yag lain). Ingatlah ini jika Anda mendapatkan program yang berbeda pada waktu menjalankan suatu program di kemudian hari.

Sebagai Image

Dengan asumsi bahwa Anda tidak mempunyai program yang menyamar, Windows XP akan mulai membuat "proses" untuk file executable. Ini meliputi pengalokasian sejumlah ruang memory kepada program itu sendiri dan menjalankan file sebagai "image", memberikan sebagian kecil RAM untuk bekerja, dan membuat sejumlah tabel untuk membantu pengaturan program pada waktu berjalan.

Bahkan proses yang sudah komplit pun tidak akan melakukan apa-apa di dalamnya. Dalam istilah Windows, proses hanyalah sebagian kecil potongan memory dan beberapa data. Software hanya dapat dijalankan dalam Windows dengan "thread", jadi thread awal dibuat dan dialokasikan ke proses.

Bagian operating system yang bertanggung jawab untuk semua ini adalah Kernel32.dll, dan tugasnya sekarang sudah selesai. Executable yang hampir siap tersebut diberikan kepada Client Server Runtime Process (csrss.exe), yang melakukan sedikit kerja tambahan untuk memastikan supaya file dapat berkomunikasi dengan sisa Windows lainnya.

Sebagai langkah terakhir, program diinisialisasi, semua DLL yang dibutuhkan di-load, dan thread awal mulai menjalankan aplikasi Anda. Pada akhirnya kita sampai di situ, dan dengan tambahan pengetahuan ini kita dapat menginterpretasikan ulang apa yang ditampilkan pada Task Manager Windows XP.

Tutup semua yang berjalan pada PC Anda, dan sisakan satu jendela Explorer. Sekarang tekan Ctrl+Alt+Del untuk membuka Task Manager, dan klik tab Applications. Seperti yang akan Anda lihat, Task Manager menampilkan icon Explorer dengan *caption* bervariasi bergantung kepada halaman web yang sedang Anda lihat. Selain nama, tab ini sama sekali tidak menampilkan aplikasi. Anda hanya akan mendapatkan daftar jendela paling atas yang sedang dibuka, dan namanya akan bervariasi bergantung kepada caption jendela.

Siapa yang Bertanggung Jawab?

Jadi, bagaimana Anda mengetahui siapa yang bertanggung jawab atas suatu jendela? Klik kanan, pilih *Go to process* dan Task Manager akan menampilkan detail Explorer.exe. Ini lebih membantu, walaupun sekarang kita tahu bahwa proses tersebut juga tidak menjalankan apa-apa. Untuk mengetahui lebih banyak apa yang sebenarnya sedang terjadi, klik View, pilih Columns, beri tanda centang (✓) Thread Count dan kemudian klik OK. Anda akan menemukan ini lebih mendekati kebenaran.

Meskipun semua program hanya berjalan dengan satu thread, tidak ada yang bisa menghentikan mereka untuk membuatnya lagi, dan Anda akan menemukan beberapa (khususnya "System") bisa mempunyai 80 atau lebih. Ini bisa jadi tanda yang bagus. Sementara satu thread melakukan tugas yang panjang, yang lain dapat menangani *user interface*, sehingga sistem bisa tetap responsif. Hal lain yang mungkin Anda lihat pada Task Manager adalah adanya beberapa svchost.exe yang sedang berjalan, kebanyakan dengan *thread count* yang tinggi. Apa yang terjadi di situ? Baca artikel berikutnya, di mana akan kita ketahui bagaimana *service* Windows bekerja. ■

LEBIH LANJUT

- **http://www.annoyances.org/exec/forum/winxp/1066973915**
- **http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/taskman_whats_there_w.mspx**