Setelah sebelumnya kami menjelaskan bagian-bagian terpenting dari motherboard, maka kini kami akan menjelaskan lebih detail bagaimana memilih processor *core logic*, dan bonus tips pemasangan motherboard dengan baik dan aman.

Arif Yuliardi

Bagian 2 dari 2 Artikel

Motherboard A-Z

Pada edisi sebelumnya, mungkin Anda ingat bahwa bagian yang paling utama untuk menentukan motherboad adalah memiliki processor dan *core logic*. Pada kesempatan ini, kami akan menjelaskan bagaimana memilih sebuah processor dan core logic yang tepat, dan juga menjelaskan beberapa teknologi terbaru yang sudah teradopsi di dalamnya.

Bagaimana Memilih Processor?

Meski di pasaran ada banyak merk processor yang banyak beredar, namun kami mencoba menyempitkan pilihannya dengan membaginya menjadi dua bagian. Hal ini berdasarkan ketersediaan dan kebutuhan. Bagian yang pertama adalah processor Intel Pentium 4 family dan yang kedua AMD Athlon 64 Family.

Kedua merk processor tersebut merupakan merk yang paling banyak dicari dan digunakan oleh kebanyakan orang dan keduanya memiliki beberapa fitur yang cukup berbeda. Di antaranya adalah Intel menggunakan *long instuction pipelines* yang didesain menghasilkan skala kecepatan *clock* supertinggi. Sedangkan pada AMD sendiri tidak menggunakan fitur tersebut, melainkan lebih menggunakan fitur *shorter Instruction pipelines* yang menghasilkan efisiensi yang baik namun sayangnya tidak bisa menghasilkan skala kecepatan yang tinggi. Untuk kalangan umum pastinya kedua hal tersebut akan membingungkan, karenanya kami akan mencoba menjelaskan bagaimana kelebihan dan kerurangan dari masing-masing merk processor.

Intel Pentium 4 Family

Biasa disebut Pentium 4. Meski dalam satu keluarga namun memiliki kecepatan yang berbeda-beda. Demikian juga dengan socket yang digunakan. Versi terbanyak yang digunakan Pentium 4 adalah menggunakan socket 478. Pada versi terbarunya telah menggunakan socket LGA 775 untuk mendukung beberapa motherboard keluaran terbaru.

Prescott

Merupakan generasi pertama Pentium 4 yang memiliki 1 MB L2 cache dan memiliki kecepatan 3,8 GHz. Namun, pada processor ini memiliki kendala yang cukup signifikan, yaitu memiliki panas yang cukup tinggi. Dan processor ini belum mendukung *operating system* dan aplikasi 64-bit. Segi baiknya, processor ini memang memiliki kinerja yang baik untuk menunjang kebutuhan multiaplikasi dan *gaming*.

Pentium 4 Extreme Edition

Merupakan jajaran processor premium dari Intel, untuk CPU desktop PC. Yang terbaru juga telah menggunakan socket LGA 775 dan berjalan di atas 3,46 GHz dengan fitur 512 K L2 cache ditambah dengan 2 MB L3 cache dan FSB sebesar 1066 MHz. Ia juga tersedia dalam versi 64-bit CPU.

Pentium D

Keluarga CPU Intel yang memiliki arsitektur dual-core. Beberapa seri yang sudah tersedia, di antaranya Pentium D 840, 830, dan 820 yang memiliki clock dari 2,80 sampai 3,20 GHz dengan FSB 800 MHz. Dengan L2 cache yang dimilikinya 2x1 Mb. Dengan dual-core, diharapkan mampu melakukan pemrosesan data dengan waktu yang lebih singkat. Selain itu, processor ini

telah dilengkapi dengan EMT64T (Extended Memory 64 Technology) yang mendukung operating system dan aplikasi 64-bit.

Jika Anda tertarik untuk membeli processor keluaran Intel, agaknya jajaran processor Pentium D adalah pilihan ideal. Dual-core dan dukungan 64-bit menjadi alasan utama. Karena ke depannya semua aplikasi dan operating system akan menggunakan 64-bit. Di samping harga jual processor ini terbilang cukup relevan, yaitu sekitar US$279.

AMD Athlon 64 Family

AMD memiliki tiga jenis processor dengan performa yang berbeda. Yaitu, Athlon 64 dan FX Series, juga Sempron. Meski dari ketiganya memiliki *basic* teknologi yang sama, namun beberapa fitur dan harga yang ditawarkan memiliki perbedaan yang cukup berarti. Pada dasarnya, processor AMD Athlon 64 mampu menghasilkan kecepatan yang tinggi terhadap aplikasi yang menggunakan banyak *floating point* dan kebutuhan *bandwidth* yang besar. Mengapa demikian?

AMD Athlon 64

Pada processor ini memiliki dua versi. Versi yang pertama yang masih menggunakan memory *single-channel*. Yaitu Athlon 64 yang menggunakan socket 75.

Sedangkan yang kedua menggunakan socket 939 dan sudah memiliki teknologi memory dual-channel. Untuk harga, sudah barang tentu Athlon 64 754 memiliki harga yang lebih murah dibanding 939. Keduanya memiliki L2 cache sebesar 1 MB, sedangkan untuk kecepatan yang ditawarkan beragam, mulai dari 2,4 GHz sampai dengan 3,0 GHz.

Athlon 64 FX

Processor ini merupakan processor yang paling tepat untuk menunjang para *gamer*, karena selain dilengkapi dengan L2 cache sebesar 1 MB dengan kecepatan terendah yang ditawarkan sebesar 2,6 GHz. Pada processor keluaran AMD baik Athlon 64 ataupun Athlon 64 FX sudah mendukung aplikasi dan operating system 64-bit. Dan kini AMD telah mengeluarkan processor dual-core, yaitu AMD Athlon 64 X2, masih menggunakan socket 939.

Core Logic Chipset

Seperti yang telah kami sebutkan di awal, salah satu bagian untuk memilih motherboard selain menentukan processor yang digunakan, core logic chipset juga bagian yang tidak kalah penting untuk dipertimbangkan. Mengapa demikian?

Jika diumpamakan sebuah motherboard adalah kota, maka core logic chipset merupakan pemerintah lokal yang melakukan pengaturan alur informasi. Chipset memiliki tugas yang amat vital. Ia akan memerintahkan apa yang harus dilakukan oleh port USB, juga menentukan seberapa cepat sistem mengakses memory. Dengan demikian fungsi dari core logic chipset sangatlah penting untuk menunjang kinerja komputer.

Sekarang ini, beberapa motherboard menggunakan dua skenario yang cukup berbeda. Skenario pertama adalah motherboard yang didesain untuk processor Intel Pentium 4. Masih mengadopsi cara lama, yaitu menggunakan memory controller yang tertanam di dalam chipset *nortbridge*.

Pada skenario ini, chipset pada motherboard bertugas sekaligus sebagai memory controller yang merupakan mesin pengontrol untuk mengatur semua kebutuhan yang ada. Memory controller terletak di dalam chipset *northbridge* yang berada dengan jarak yang relatif tidak terlalu jauh dari processor. Tujuannya untuk menghasilkan bus bandwidth memory yang besar.

Skenario yang kedua adalah motherboard untuk AMD Athlon 64, Athlon 64 FX dan Athlon 64 X2 yang memiliki perbedaan jauh dengan Intel. Pada motherboard AMD Athlon 64, memory controller tidak lagi terdapat pada nortbridge chipset, melainkan dipindahkan ke dalam processor.

Pada kondisi ini, bus memory controller bisa sama cepat dengan kecepatan core processor. Dengan demikian, menjadikan sebuah pasangan gigahertz yang cepat sehingga mampu menghasilkan kinerja yang jauh lebih cepat ketimbang skenario yang pertama.

Namun,ini bukan merupakan kemenangan secara mutlak, karena besarnya

Beberapa processor terbaru yang sudah mendukung 64-bit dan dual-core.

performa yang dimiliki oleh AMD memiliki kekurangan dalam fleksibilitas.

Intel memang memiliki fleksibilitas yang cukup baik. Contohnya jika Anda sekarang membeli processor Intel Pentium 4, Anda bisa menggunakan processor tersebut pada motherboard yang menggunakan DDR400. Demikian juga untuk motherboard DDR2/800 bahkan untuk motherboard DDR3, yang akan segera diluncurkan.

Hal tersebut tidak terjadi jika Anda menggunakan processor AMD Athlon 64 ataupun 64 FX karena controller-nya terikat pada satu teknologi memory saja. Sehingga Anda harus menyesuaikan memory yang Anda gunakan sesuai dengan controller yang terdapat secara terintegrasi di dalam processor.

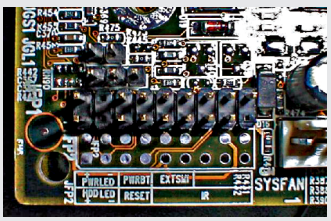
Itulah salah satu alasan kenapa sampai sekarang ini AMD masih mengadopsi teknologi memory DDR 400. Karena selain ingin tetap memberikan fleksibilitas terhadap konsumennya, AMD juga beranggapan kemampuan bandwith memory yang dihasilkan DDR

TIPS PEMASANGAN MOTHERBOARD

Memasang motherboard bukanlah sesuatu yang sulit. Tidak diperlukan ijasah ataupun kecerdasan jenius untuk dapat melakukannya. Melainkan hanya perlu membutuhkan ketelitian dan kemauan. Untuk melakukan hal tersebut, akan kami berikan panduan untuk Anda.

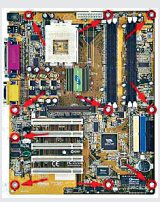
1. Perhatian khusus untuk jumper.

Sampai sekarang ini memang tidak ada standar *layout* untuk jumper pada motherboard. Hal ini dikarenakan industri produsen motherboard, memiliki desain layout tersendiri. Meskipun tidak mencolok antara masing-masing produsen. Namun, untuk Anda yang baru kali pertama memasang motherboard, kami sarankan untuk membaca buku manualnya. Karena tidak semua produk motherboard, memiliki penjelasan text yang tertera jelas pada PCB motherboard. Jangan menebak-nebak untuk hal ini.



2. Teknologi sekrup.

Cukup sulit untuk menentukan kategori yang tepat untuk hal ini. Sebelum memasang motherboard, kebanyakan casing dilengkapi sekrup yang cukup banyak. Optimalkan penggunaannya. Usahakan semua titik lubang pengikat motherboard terpasang sekrup. Dengan demikian, motherboard dapat terpasang dengan lekat di casing. Namun tentunya jangan asal pasang. Sesuaikan panjang dan ukuran sekrup sesuai dengan lubang yang digunakan.



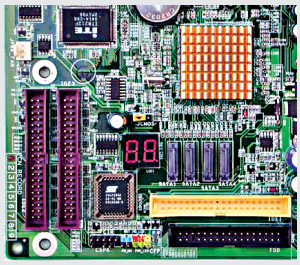
3. Gunakan I/O Shield.

Sebuah plat besi yang berfungsi untuk menutup celah yang terdapat antara input/ouput konektor dari motherboard. Dengan memasangkan plat besi tersebut, selain komputer akan terlihat rapi, komputer juga akan lebih tertutup sehingga tidak dimasuki oleh kotoran atau serangga.

I/O Shield biasanya disediakan pada paket penjualan sebuah motherboard. Bentuknya yang spesifik, disesuaikan dengan ketersedian I/O pada produk motherboard yang bersangkutan. Sebaiknya jangan menggunakan I/O shield untuk motherboard lain, karena dapat menghalangi I/O yang tersedia.

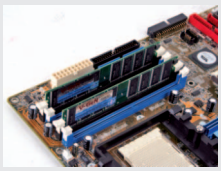
4. Pilih port yang tepat.

Asumsi bahwa dengan memasangkan SATA atau PATA drive ke dalam sembarang konektor akan membuat sistem Anda bisa *booting*. Beberapa motherboard menyediakan RAID controller untuk SATA/PATA. Untuk ini, membutuhkan driver yang biasanya disertakan dalam sebuah



disket. Anda harus menginstalnya terlebih dahulu baru Windows XP Anda bisa booting. Anda juga harus melakukan setting-an terlebih dahulu dari dalam BIOS dan mengalamatkan RAID untuk bisa digunakan pada harddisk PATA.

5. Sesuaikan RAM.



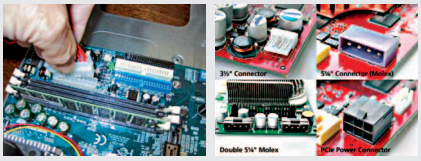
Sebelumnya banyak orang yang mengatakan bahwa untuk menjalankan *dual-channel*, cukup dengan cara memasang memory sesuai dengan warnanya. Jika Anda memasang memory pertama pada slot berwarna biru, memory kedua pun harus demikian. Namun bagaimana jika motherboard tersebut memiliki 4 slot memory dengan warna yang sama? Jawabannya bisa Anda temukan pada buku manual motherboard tersebut. Jika Anda tidak mendapatkan konfigurasi yang tepat untuk dual-channel memory tersebut, kemungkinan besar sistem akan mengalami penurunan kinerja yang cukup signifikan.

6. Gunakan power konektor yang sesuai.

Pada motherboard keluaran terbaru menggunakan konektor yang berbeda

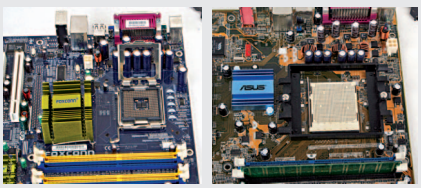
400 masih mampu menangani semua kebutuhan proses *computing* saat ini.

Meskipun semua chipset mengacu pada memory controller, namun core logic chipset sendiri memiliki beberapa fungsi yang sangat penting. Yaitu performa USB, harddisk, dan seberapa cepat PCI dan VGA slot (AGP atau PCIe x16) dapat mentransfer data.



dengan yang terdahulu (lihat artikel bagian 1). Oleh karena itu, pasang semua konektor power yang ada sesuai dengan yang terdapat di motherboard, jangan pernah menggabungkan dua power ke dalam satu konektor, karena bisa menyebabkan kerusakan yang fatal.

7. Pemasangan processor.
Ini adalah bagian yang tersulit dalam pemasangan motherboard. Karena jika Anda salah memasangnya bukan tidak mungkin processor Anda akan rusak. Pada motherboard lama, Anda membutuhkan alat bantu obeng untuk melepaskan pengait heatsink. Dan tak sedikit yang memiliki tingkat kesulitan yang tinggi. Karenanya jika Anda masih menggunakan motherboard dengan socket lama (Socket A, dan socket 478) harus berhati-hati. Pada motherboard sekarang (socket 775, 754, dan 939) bisa dibilang bisa langsung dipasang tanpa harus menggunakan alat bantu obeng. Pengait heatsink jauh lebih mudah dioperasikan, dibanding processor jaman dulu.



Perkembangan Chipset Terakhir

- **Intel**
  Untuk Intel sekarang ini telah meluncurkan motherboard dengan chipset 955X dan 945P yang mendukung DDR2/667, dan secara tegas meninggalkan DDR400. Namun pada chipset ini, hal yang paling diunggulkan adalah kemampuan chipset mendukung fitur dual-core processor.
- **nVIDIA**
  Setelah sebelumnya sempat berseberangan dengan Intel, kini chipset nVIDIA bisa bersanding dengan processor Intel. Dengan mencoba mengeluarkan chipset terbarunya yaitu nVIDIA nForce4 Intel Edition. Chipset serupa sebelumnya hadir untuk basis Athlon 64. Pada chipset tersebut telah mendukung teknologi SLI dan dilengkapi dengan SATA 3 GB juga Firewall. Namun sayangnya, belum ada kepastian dari nVIDIA, mengenai dukungan chipset tersebut untuk dual-core processor.
- **VIA**
  Meski produsen yang satu ini terbilang lambat mengembangkan teknologi ketimbang kedua produsen yang telah kami sebutkan di atas, namun VIA telah mengeluarkan VIA PT984 Pro. Keunikan chipset ini adalah dapat menjalankan video card PCI Express x16 juga AGP 8x. Keduanya dapat berjalan secara simultan dan mendukung dual monitor. Namun, hal tersebut berbeda dengan SLI. Karena pada konfigurasi SLI, mampu membagi bandwidth data dari dua buah video card. Selain itu, VIA memberikan dua pilihan memory yaitu DDR400 dan DDR2 667 sehingga bisa menyesuaikan dengan kebutuhannya.

Setelah sebelumnya kami berikan beberapa tip untuk memilih processor, maka kami akan memberikan juga kepada Anda bagaimana memilih chipset yang tepat.

- Hal pertama yang Anda harus perhatikan adalah jenis chipset yang digunakan. Jangan terkecoh dengan nama-nama produk yang unik. Beberapa produsen sengaja menggunakan nama yang unik untuk menarik pembeli. Namun tidak jarang hasil dan kinerja yang dimilikinya kurang sesuai dengan namanya.
- Perhatikan kecepatan interkoneksi antara chipset northbride dengan southbridge. Kecepatannya minimal menggunakan 133 MB/s. Beberapa produk terbaru sudah bisa mencapai 2 GB/s. Mana yang harus dibutuhkan, itu adalah sebuah pertanyaan yang sulit. Untuk kebutuhan 'normal' 800 MB/s hingga 1 GB/s terbilang cukup memadai. Anda juga butuh pertimbangan untuk konfigurasi chipset jika ada 4 PCI Express X1 dalam sebuah sourthbridge, Anda akan membutuhkan 1-2 GB/s koneksi untuk mendukung bandwidth yang sesuai, namun jika hanya ada X1 jalur yang terhubung langsung ke northbridge, maka interkoneksi tersebut belum Anda butuhkan.
- Perhatikan chipset southbrigde, produsen motherboard dapat dengan mudah menukar chipset tersebut dengan chipset yang lain. Dan jika hal tersebut terjadi, maka beberapa fitur yang dimiliki akan lebih sedikit dan terbatas. Karenanya Anda harus memperhatikan dengan benar.
- Sama halnya dengan memilih motherboard, untuk memilih chipset yang tepat Anda juga membutuhkan *second opinion* untuk memberikan referensi yang tepat. Karenanya Anda bisa mendapatkan dari beberapa *review* pada media tentang chipset tersebut agar Anda tidak menyesal di kemudian hari.

Setelah semuanya kami jelaskan, maka tinggal Anda yang menentukan pilihan dan selamat membangun komputer baru. Semoga dengan panduan ini, Anda tidak terjebak dalam memilih. ■

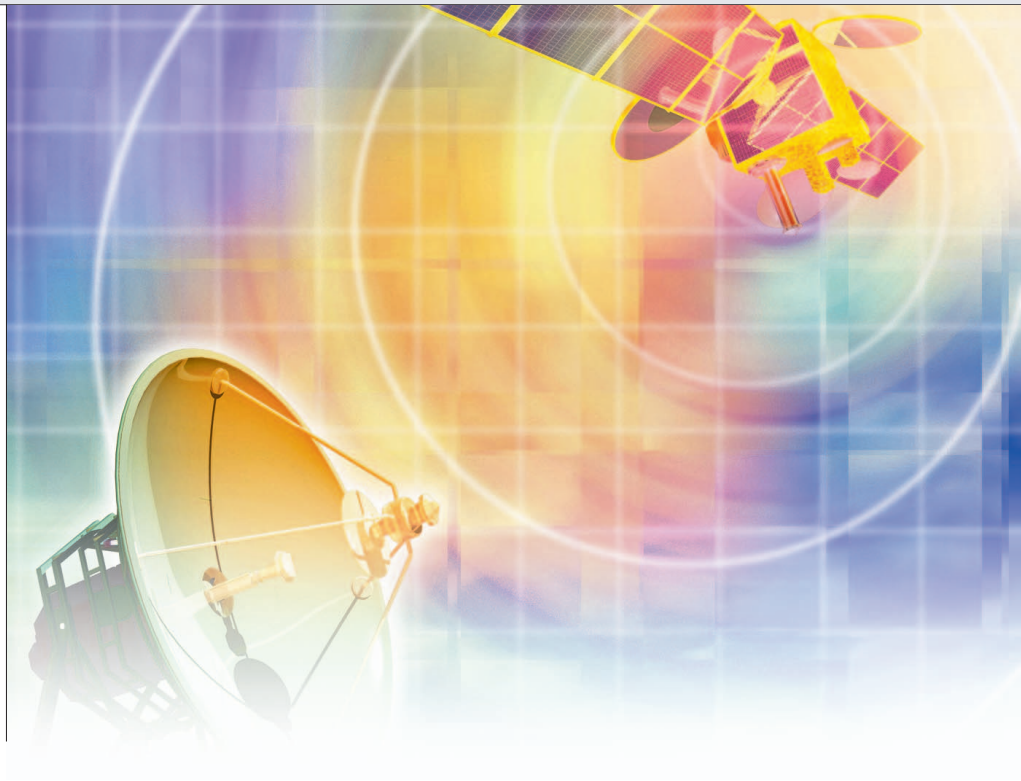
LEBIH LANJUT

- **www.intel.com**
- **www.ati.com**
- **www.nvidia.com**
- **www.amd.com**
- **www.sis.com**
- **www.via.com.tw**

Solusi komunikasi data berkecepatan tinggi dengan harga relatif tidak mahal tidak hanya terbatas pada Cable modem dan ADSL saja, media-media komunikasi seperti *wireless* dan satelit juga dapat Anda nikmati untuk itu.

Hayri

Bagian 2 dari 2 Artikel



Kenali Broadband Lebih Jauh

Seperti telah dibahas pada artikel sebelumnya ("Kenali Broadband Lebih Jauh Bagian 1 dari 2 Artikel"), koneksi *broadband* tidak terbatas pada jenis media dan lokasi di mana koneksi tersebut berada. Selama suatu lokasi dapat dilalui oleh media komunikasi, koneksi broadband mungkin saja dibuat pada lokasi tersebut.

Teknologi ADSL dan Cable yang telah dibahas sebelumnya memiliki kelemahan yang sangat mencolok, yaitu masalah jarak dan lokasi pemasangannya. Teknologi ADSL sangat terbatas jarak tempuh medianya, yaitu hanya sekitar 5 kilometer maksimal. Sedangkan teknologi Cable masih sangat terbatas penyebaran medianya sehingga lokasi-lokasi tertentu belum memungkinkan untuk menggunakan media jenis ini.

Teknologi broadband yang kali ini akan dibahas adalah teknologi yang tidak melibatkan kabel sebagai media pembawanya, namun menggunakan sinyal radio dan frekuensi. Dengan adanya koneksi broadband dengan menggunakan media *wireless*, pengguna akan lebih mudah untuk menikmati cepatnya berkomunikasi dengan lawannya, baik melalui Internet maupun melalui jaringan lokal.

3. Teknologi Satelit Broadband

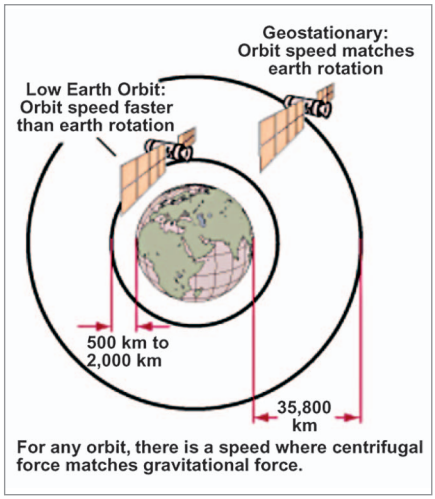
Komunikasi via benda luar angkasa yang bernama satelit ini telah lama ada. Problem paling penting yang dapat diselesaikan oleh teknologi komunikasi via satelit ini adalah teknologi satelit dapat memberikan *bandwidth* relatif cukup besar untuk lokasi-lokasi yang sama sekali tidak memiliki infrastruktur untuk itu.

Lokasi-lokasi yang tidak dapat terjangkau oleh kabel, wireless, dan teknologi komunikasi lainnya seperti di tengah hutan rimba, di tengah lautan, di daerah terpencil pegunungan, dan banyak lagi, masih memungkinkan untuk dijangkau oleh satelit. Satu-satunya cara untuk mendapatkan koneksi broadband yang relatif cepat pada lokasi seperti ini tidak lain adalah menggunakan media komunikasi satelit dua arah.

Penggunaan media satelit untuk komunikasi data pada awal-awal perkembangannya hanya digunakan untuk melewatkan data *downstream* saja (arah data hanya datang dari luar menuju ke jaringan Anda, tidak bisa mengirim data keluar). Atau dengan kata lain satelit hanya menyediakan komunikasi asimetrik satu arah saja. Bagaimana dengan proses pengiriman datanya? Biasanya data yang ingin dikirim dilewatkan melalui media lain seperti *dial-up*, ISDN, dan banyak lagi. Namun untuk saat ini, teknologi satelit sudah dapat memberikan servis komunikasi dua arah, jadi Anda tidak perlu repot-repot mengakalinya.

Layanan media satelit rumahan sederhana saat ini dapat menghantarkan data dengan kecepatan downstream hingga 1,5 Mbps dan kecepatan upstream data hinga 125 Kbps. Aktivitas yang banyak dalam jaringannya dapat mempengaruhi kecepatan transfer yang dihantarkan satelit. Perangkat komputer yang terhubung dengan satelit tidak perlu melakukan transaksi *login* apapun seperti halnya komunikasi melalui *dial-up*.

Melihat sifat alamiah komunikasi satelit yang bersifat asimetris ini (kecepatan transfer *downstream* lebih besar dari upstream), beberapa aplikasi komunikasi data tidak cocok untuk menggunakan media ini karena tidak dapat bekerja dengan baik. Aplikasi



Jarak tempuh data dari lokasi pengguna menuju ke satelit penghubung sangat berpengaruh terhadap *bandwidth*, kecepatan transfer dan latensi dari komunikasi data yang Anda lakukan.

seperti VoIP tidak akan bisa berjalan dengan sempurna jika menggunakan komunikasi satelit. Maka itu, aplikasi data lebih cocok menggunakan satelit daripada aplikasi suara.

Satelit yang umumnya digunakan dalam komunikasi saat ini adalah satelit Geostationary Orbit Satellite (GSO) dan Non-Geostationary Orbit Satellite (NGSO). Satelit yang termasuk dalam golongan NGOS adalah Low-Earth-Orbih satellite (LEO). Satelit yang termasuk dalam kategori LEO berjarak sekitar 500 sampai 2000 kilometer dari permukaan bumi.

Satelit yang biasanya digunakan untuk komunikasi data broadband adalah satelit yang mengorbit pada jarak sekitar 35,888 kilometer (22,300 mil) dari atas garis katulistiwa atau masih tergolong dalam satelit jenis GSO. Untuk masalah latensinya, satelit yang tergolong dalam satelit GSO lebih besar latensinya daripada satelit dalam golongan LEO. Hal ini disebabkan jarak orbit geostasionernya jauh lebih besar. Latensi semakin membesar disebabkan jarak tempuh data yang semakin jauh.

Layanan media komunikasi satelit rumahan yang sederhana kali pertama digunakan pada tahun 1980-an dengan sebutan "*backyard dishes*". Jenis dish atau piringan satelit yang paling umum digunakan untuk keperluan komunikasi data broadband yang paling tidak membutuhkan dish satelit berukuran kecil dengan diameter sekitar 1.2 meter (3.9 feet). Dish ini berfungsi sebagai mediator penangkap dan pengirim sinyal komunikasi. Selain itu, sepasang kabel koaksial standar juga diperlukan untuk menyambungkan dish satelit dengan modem satelit. Modem satelit berfungsi untuk mengubah sinyal-sinyal "mentah" yang diterima satelit menjadi sinyal yang dimengerti oleh sistem komputer Anda.

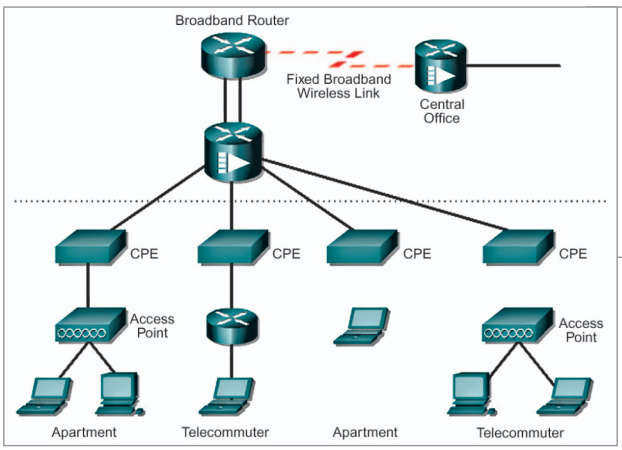
Modem ini juga berfungsi sebagai pengubah sinyal-sinyal digital komputer menjadi sinyal komunikasi antarsatelit. Modem ini biasanya memiliki dua *interface* untuk menghubungkan antara dish satelit dengan perangkat komputer Anda. Teknologi *interface* menuju ke perangkat komputer juga bermacam-macam, ada yang berbentuk Ethernet (konektor RJ45), ada yang berbentuk port serial, port USB, dan banyak lagi. Teknologi satelit yang terbaru bahkan dapat menggunakan ukuran dish yang lebih kecil dan memungkinkan para pelanggannya untuk melakukan komunikasi data melaluinya sambil juga menerima siaran televisi yang memang dipancarkan untuknya.

4. Teknologi Fixed-Wireless Broadband

Teknologi wireless yang sering digunakan untuk proses komunikasi data atau suara yang sifatnya tidak banyak mobilitasnya sering disebut dengan istilah *fixed wireless*. Anda dapat membedakan dengan mudah antara fixed-wireless dengan mobile-wireless karena masing-masing memiliki sistem kerjanya sendiri. Komunikasi data yang menggunakan media fixed wireless maupun mobile wireless saat ini memang sedang *booming*. Namun untuk menghantarkan servis broadband, pilihan banyak jatuh pada jenis media fixed wireless broadband. Alasannya pun banyak macam, ada yang memilih karena harganya yang murah, ada yang memilih karena lokasi geografisnya yang sangat cocok untuk menggunakan wireless yang tidak membutuhkan mobilisasi, dan banyak lagi. Sebenarnya sistem fixed wireless ini telah memiliki sejarah yang cukup panjang.

Komunikasi *point-to-point* menggunakan teknologi microwave untuk dilewatkan data dan suara telah lama digunakan oleh masyarakat. Koneksi jenis ini juga dapat dikategorikan sebagai media fixed wireless. Namun, teknologi terus berkembang semakin canggih dan *advance*, sehingga memungkinkan penggunanya menggunakan frekuensi yang lebih tinggi dengan material-material untuk komponen antena yang lebih canggih. Sebagai hasil dari perkembangan ini adalah antena yang berukuran lebih kecil dengan bandwidth yang lebih tinggi dapat digunakan untuk berbagai keperluan komunikasi saat ini, baik data maupun suara.

Apa untungnya dengan ukuran antena yang semakin mengecil? Antena yang kecil ukurannya akan berdampak pada harga kepemilikan dan penggunaan sistem fixed wireless ini menjadi lebih murah dari sebelumnya. Selain itu, ukuran yang tidak terlalu besar juga akan memudahkan pengguna untuk memasang, mengatur dan melakukan *troubleshooting*. Atas dasar inilah teknologi fixed wireless kini banyak dipilih oleh pengguna sebagai media komunikasi *last mile* mereka baik untuk



Komunikasi data kategori "Broadband" pada dasarnya tidak mengenal jenis media, asalkan memiliki jalur transportasi data yang cukup lebar dan dapat didistribusikan ke banyak pengguna, maka jadilah layanan *broadband*.

Internet maupun untuk ke kantor-kantor cabang mereka.

Namun, teknologi fixed wireless pada umumnya sangat terpengaruh oleh faktor jarak dan kondisi lingkungan di mana media ini berada. Jarak antara pengirim dan penerima data yang menggunakan fixed wireless sangat terbatas dan cukup berpengaruh terhadap bandwidth yang mampu dihantarkannya. Semakin jauh jarak tempuh data, biasanya semakin kecil pula bandwidth yang bisa diberikannya begitupun sebaliknya.

Kondisi lingkungan juga sangat berpengaruh terhadap komunikasi jenis ini. Lingkungan yang banyak dilalui oleh frekuensi-frekuensi yang sama dengan yang digunakan perangkat Anda tentu akan mengakibatkan gangguan dalam proses komunikasi. Lingkungan yang banyak halangannya di tengah-tengah proses komunikasi perangkat fixed wireless ini juga tidak baik untuk kelangsungan proses komunikasi. Maka itu, teknologi ini harus digunakan dengan perencanaan dan survai yang tepat.

Segmen pasar dari teknologi fixed wireless ini dapat digolongkan menjadi empat bagian yang umum, yaitu:

- **Local Multipoint Distribution Service (LMDS)**

LMDS adalah sebuah sistem komunikasi menggunakan gelombang radio yang kali pertama dibangun oleh Bellcore. Sejak kali pertama digunakan oleh perusahaan tersebut, teknologi ini memang sudah berperan sebagai media *local loop* yang ditargetkan untuk penggunaan pada area-area di mana penarikan kabel tidak dimungkinkan.

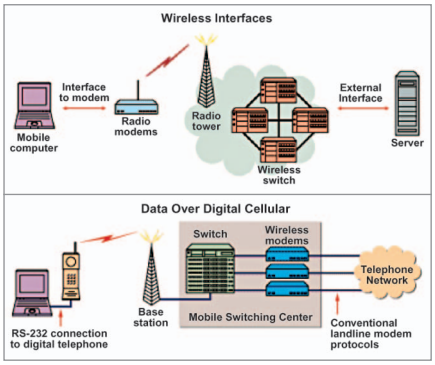
LMDS memang tidak bisa dibandingkan kecepatan dan reliabilitasnya dengan media fiber optic, namun teknologi ini dapat menyediakan solusi paling ekonomis untuk memenuhi kebutuhan koneksi berkecepatan tinggi dengan jarak tempuh yang cukup jauh. Vendor Alcatel yang juga membangun teknologi ini memberinya nama "Wireless IP".

LMDS menggunakan sistem komunikasi radio *point-to-multipoint* untuk membangun komunikasi dari perangkat pemancar (*Base Station Unit*) ke perangkat pelanggan (*Subscriber Unit*). Sedangkan komunikasi dari SU ke BSU menggunakan sistem komunikasi Point-to-Point. Frekuensi yang digunakan untuk memenuhi kebutuhan LMDS adalah 27.5 GHz-28.35 GHz, 29.1 GHz-29.25 GHz, 31.075GHz-31.225 GHz, 31.Ghz-31.075Ghz, dan 31.225 GHz-31.3 GHz.

Jarak tempuh teknologi LMDS yang maksimal adalah sekitar 5 km dengan bandwidth yang mencapai di atas T3 (45 Mbps). Spesifikasi seperti ini sangat cocok digunakan untuk keperluan perusahaan menengah hingga besar. Teknologi wireless-nya membuat teknologi ini menjadi sangat berguna di daerah-daerah yang tidak ada media komunikasi via kabelnya.

- **Multichannel Multipoint Distribution Service (MMDS)**

MMDS adalah sebuah teknologi microwave yang pada awalnya didesain untuk keperluan transmisi satu arah saja. Biasanya MMDS digunakan untuk memancarkan siaran TV cable bagi daerah-daerah yang tidak memungkinkan untuk dipasangi kabel-kabel. Maka dari itu, banyak yang menyebut teknologi yang satu ini dengan julukan "wireless cable". MMDS menggunakan frekuensi UHF (*Ultra High Frequency*) dalam membangun komunikasinya yaitu sekitar 2.5 sampai dengan 2,683 GHz.



Desain komunikasi yang menggunakan *interface wireless* memiliki desain yang hampir sama secara umum. Yang membedakannya hanyalah cara pengguna akhirnya melakukan proses komunikasi tersebut. *Fixed wireless* dan *mobile wireless* dapat Anda bedakan dengan mudah.

Antena yang banyak digunakan oleh teknologi MMDS.

Baru pada tahun 1998, organisasi penciptanya, FCC, membuatkan teknologi ini memiliki kemampuan berkomunikasi dalam dua arah. Sejak saat itulah, teknologi ini banyak digunakan untuk membawa data yang memerlukan proses komunikasi dua arah, seperti komunikasi data LAN, Internet, bahkan VoIP. Servis dari teknologi MMDS ini sangat ideal digunakan oleh pengguna rumahan. Hal ini dikarenakan data rate yang mampu dihasilkan juga tidak terlalu besar dan harga kepemilikan yang relatif murah untuk pengguna rumahan atau SOHO.

Teknologi MMDS memiliki jarak tempuh media pada spesifikasi maksimal adalah sebesar 56,3 km dengan *throughput* yang tidak jauh berbeda dengan koneksi DSL dan Cable. MMDS memang teknologi yang ditargetkan untuk pengguna SOHO maupun pengguna rumahan.

- **License-free Industrial Scientific and Medical (ISM) Band**

Sesuai dengan namanya, *Lisence-free*,

Modem dan *dish* satelit yang kini sudah jauh lebih simpel dan kompak bentuknya membuat teknologi ini semakin nyaman digunakan.

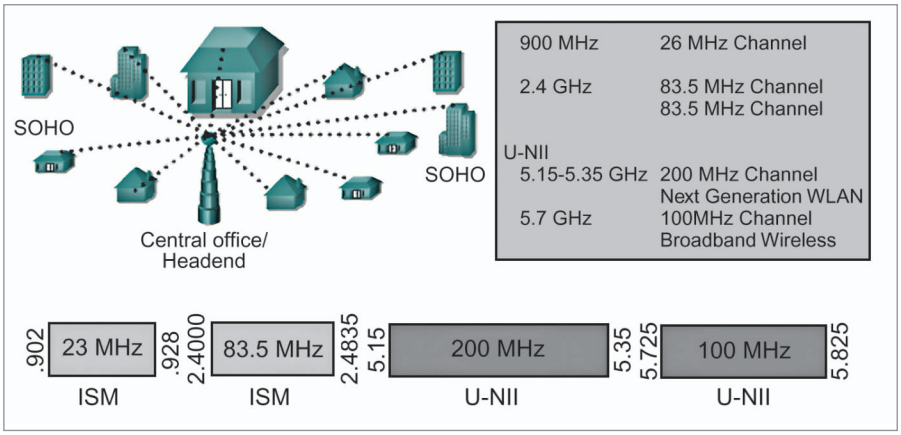
biasanya segmentasi pasar yang menggunakan frekuensi ini akan terbebas dari biaya untuk membuat izin penggunaan frekuensi komunikasinya. Frekuensi-frekuensi yang termasuk dalam jenis ini tidak standar di semua negara, karena masing-masing negara memiliki peraturannya sendir-sendiri. Di Indonesia salah satu frekuensi yang dibebas-biayakan adalah frekuensi 2.4 GHz yang sudah sangat banyak penggunanya.

Segmen License-free ISM biasanya mampu membangun komunikasi sejauh 4,8 km hingga 40 km dengan throughput mulai dari 64 Kbps hingga 53 Mbps, tergantung pada frekuensi berapa dan teknologi apa yang digunakan dan banyaknya pengguna yang terkoneksi dalam frekuensi tersebut.

Keuntungan dari mengunakan teknologi ini adalah Anda akan berhemat uang yang cukup bayak karena tidak perlu keluar uang untuk mendapatkan dan menggunakan izin frekuensi. Kerugian dari menggunakan teknologi ini karena terlalu banyak penggunanya, maka sangat rentan terhadap gangguan interferensi sinyal komunikasi yang Anda gunakan. Gangguan interferensi terjadi ketika satu atau lebih sinyal yang menggunakan frekuensi yang sama melewat jalur komunikasi yang sedang Anda gunakan yang juga dalam frekuensi yang sama dengan sinyal lain. Isu interferensi ini sangat meluas seiring dengan penggunaan *lisence-free service* ini.

- **Unlicensed National Information Infrastructure (U-NII) Band**

Segmentasi pasar yang satu ini ditujukan untuk penggunaan dalam jarak pendek, kecepatan tinggi dengan harga penggunaan yang relatif murah. Teknologi U-NII terdiri atas tiga pita frekuensi yang semuanya berada di dalam frekuensi rage 5 GHz. Ketiga frekuensi tersebut adalah 5,15 GHz-5,25 GHz, 5.23 GHz-5.35 GHz, dan 5,725 GHz-5,825. Penggunaan frekuensi U-NII tidak memerlukan perizinan di beberapa tempat.



Anda bebas memilih frekuensi berapa yang ingin Anda gunakan selama frekuensi itu masih termasuk dalam *free* frekuensi.

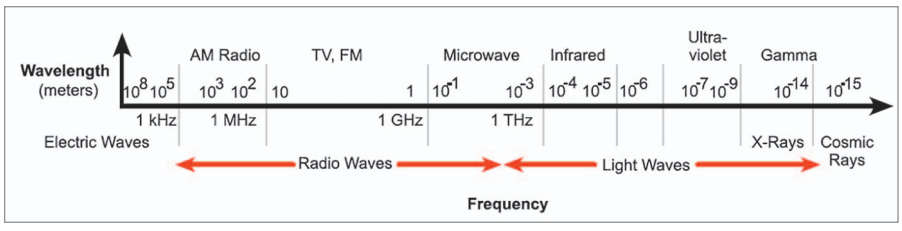
Teknologi dan pasar dari media komunikasi wireless tidak hanya terbatas pada apa yang disebutkan di atas saja. Selain itu, masih ada teknologi yang cukup reliabel yaitu teknologi wireless melalui sinar Laser. Komunikasi yang dibangun oleh media laser sangat reliabel. Untuk membangun koneksi laser hal pertama yang dibutuhkan adalah lokasi kedua titik yang harus LOS (*Line OF Sight*). Artinya, jarak yang dapat ditempuh oleh sinar ini tidak bisa terlalu jauh. Jarak ideal sinar laser untuk dapat membangun komunikasi jarak jauh adalah sekitar 5 kilometer. Bandwidth yang bisa diberikan pun sangat bervariasi, mulai dari 64 Kbps sampai dengan 45 Mbps dapat dilayani oleh laser.

Penggunaan sinar laser untuk membawa data memang banyak memberikan keuntungan. Menggunakan sinar laser Anda tidak memerlukan perizinan apapun, jadi Anda dapat menggunakan kapanpun dan di manapun. Media laser juga cukup aman karena tidak mudah untuk didengarkan oleh orang lain. Dengan adanya penghalang sedikit saja pada perjalanan sinarnya, maka koneksi menjadi terganggu. Ini bisa menjadi indikator apakah ada orang iseng yang sengaja bermain di tengahnya atau tidak.

Meskipun hebat laser bukan tanpa kelemahan. Media jenis ini sangat rentan terhadap kelembaban udara. Jika lensa lasernya lembab dan berembun, maka komunikasi menjadi sangat terganggu. Selain itu, laser juga rentan terhadap getaran dan burung-burung yang sering kali menghalangi sinar komunikasi dari perangkat laser tersebut. Jaraknya juga tidak terlalu jauh untuk dapat melayani banyak pengguna. Maka dari itu, media wireless tidak digunakan dalam menghantarkan servis broadband.

Koneksi Broadband Pilihan Anda

Anda bebas memilih jenis koneksi apa yang sangat cocok untuk kebutuhan Anda. Dengan distribusi bandwidth yang dibuat bersistem broadband, semua media komunkasi ini menjadi semakin meluas penggunaannya tidak hanya terbatas pada satu pengaplikasian saja. Media wireless yang ditumpangi teknologi broadband memang jauh lebih fleksibel penggunaannya dibandingkan dengan ADSL dan Cable. Namun, semua kelemahan teknologi ini juga masih tetap ikut diwariskan ke dalam koneksi wireless broadband access. Jadi, terserah Anda mau pilih yang mana? ■



Frekuensi komunikasi tidak bisa sembarangan digunakan karena memang diatur dalam mendapatkan perizinannya.

LEBIH LANJUT

- **http://www.starband.com/**
- **http://www.cabledatacomnews.com/wireless/cmic10.html**

Banyak fasilitas yang tersedia untuk membangun koneksi *remote desktop,* namun sebelum menggunakannya pikirkan juga keamanannya agar Anda benar-benar nyaman menggunakannya.

Hayri

Bagian 2 dari 2 Artikel

Remote Desktop Aman di Windows

▶Pada edisi sebelumnya telah sedikit dibahas mengenai apa *sih* sebenarnya *remote desktop* itu, apa gunanya menggunakan fasilitas remote desktop, dan apa saja yang harus diperhatikan dalam membuat dan menggunakan fasilitas remote desktop. Selain itu, juga sudah ditawarkan sebuah solusi alternatif untuk Anda yang tidak memiliki fasilitas remote desktop yang *build-in*. Solusi ini bukan hanya menawarkan kemudahan menjalankan fasilitas remote desktop, namun juga keamanannya yang tetap dijaga.

Program-program untuk mendukung solusi ini sudah dipilih pada edisi sebelumnya, yaitu program VNC yang bertugas membangun komunikasi remote desktop, program Stunnel yang berfungsi sebagai pembuat tunnel komunikasi yang diperkuat dengan sistem keamanan SSL, dan program OpenSSL yang bertugas menyediakan fasilitas dan fungsi-fungsi enkripsi dan kriptografi sehingga dapat membentuk sistem sertifikasi penjaga keamanan data Anda.

Untuk program VNC, Anda dapat men-*download*-nya di *http://www.realvnc.com/download.html* bagian Freeware Edition. Sedangkan untuk program Stunnel dan OpenSSL, Anda dapat men-download-nya di *http://www.stunnel.org/download/binaries.html*. Jangan lupa juga untuk men-download file-file library tambahan, yaitu libeay32.dll dan libssl32.dll di situs ini.

Untuk keperluan OpenSSL, download juga file skrip yang bernama OpenSSL.conf di *http://www.securityfocus.com/data/tools/openssl.conf* dan ca.bat di situs *http://www.securityfocus.com/data/tools/ca.bat*. Setelah semuanya selesai di-download, maka pembahasan selanjutnya adalah melakukan instalasi dan pengaturan program ini agar siap digunakan.

Proses Instalasi Solusi Alternatif

Setelah Anda men-*download* semua program yang disebutkan di atas, proses instalasi program-program ini selanjutnya relatif tidak sulit, namun banyak langkah yang perlu diperhatikan. Kali pertama yang harus Anda instal adalah program VNC, kemudian Stunnel dan terakhir OpenSSL.

- **Instalasi VNC**

Instalasi dari program remote desktop sederhana ini cukup mudah, seperti halnya menginstal program-program biasa lainnya. Installah pada PC atau server Anda yang ingin dipersenjatai dengan fasilitas remote desktop. Ikuti langkah-langkah instalasinya. Setelah selesai instalasi, Anda harus melakukan registrasi servis VNC pada PC Anda. Caranya kliklah tombol *Start|Programs|RealVNC|VNC Servers|Register VNC Server Service*.

Setelah melakukan semua langkah di atas, *reboot*-lah PC Anda. Setelah di-reboot, maka jadilah VNC Server pada PC Anda. Namun pada program RealVNC versi terbaru, Anda tinggal mengaktifkan langkah registrasi di atas hanya dengan mencentang (✓) opsinya pada awal penginstalan, maka semuanya berjalan secara otomatis.

Setelah reboot, Anda masih perlu melakukan pengaturan parameter dasar dari VNC server ini. Yang pertama harus Anda buat adalah sebuah *password*. Peranan password sangatlah penting di sini karena merupakan satu-satunya kunci untuk masuk ke dalam PC Anda dan

mendapatkan akses apapun di dalamnya. Maka itu, usahakan untuk tidak membuat password yang asal-asalan. Buatlah sesulit mungkin namun masih mudah untuk Anda ingat.

Kliklah tab *Authentication* dan kliklah opsi *VNC password authentication*, kemudian kliklah tombol *Configure*. Isilah password pada jendela pengaturannya. Setelah selesai dengan password, centanglah (✓) opsi *Prompt Local user to accept connections*. Opsi ini perlu dipilih jika Anda ingin membuat server yang ingin diakses dengan VNC memberikan tanda pemberitahuan kalau ada yang ingin masuk melalui program VNC.

Setelah selesai, kliklah tab *Connections* dan hilangkanlah tanda centang (✓) untuk opsi Server Java Viewer via HTTP port :. Java Viewer tidak bisa digunakan di dalam solusi ini karena untuk membuat aplikasi berbasiskan java tampil di halaman remote Anda, dibutuhkan dua buah tunnel SSL dan itu tidak bisa diberikan oleh program Stunnel. Untuk itu, lebih baik dinonaktifkan saja.

Sisa dari pengaturan VNC hanya bersifat opsional saja. Anda dapat mengunci desktop yang Anda remote ketika Anda *disconnect* dari PC tersebut, atau langsung *logoff* atau bisa juga tidak melakukan apa-apa. Selain itu, Anda juga dapat menghilangkan wallpaper yang ada di desktop PC yang di-remote agar koneksi remote tidak terlalu berat. Atau bisa juga mengunci keyboard dan mouse pada PC yang di-remote sehingga tidak bisa diganggu oleh orang yang berada di lokasi. Selain itu, masih banyak pengaturan yang bersifat opsional lainnya. Anda dapat dengan bebas menentukan selera Anda.

- **Instalasi Stunnel**

Program Stunnel merupakan komponen yang dapat memungkinkan koneksi VNC Anda ini aman dari gangguan orang yang tidak berkepentingan. Program Stunnel seperti telah dijelaskan di atas merupakan program yang dapat menyediakan koneksi secara *tunneling*. Koneksi tunnel merupakan koneksi yang telah lama digunakan untuk membangun sebuah koneksi pribadi, namun melalui jalur umum yang dapat dilewati siapa saja. Namun yang membedakannya dengan yang lain, koneksi tunnel dalam program Stunnel ini dilengkapi dengan sistem keamanan SSL. Dengan demikian, tunnel ini cukup aman digunakan untuk melewati data-data kritikal.

Langkah instalasi selanjutnya adalah membuat fasilitas Stunnel aktif di perangkat komputer Anda. Setelah Anda men-download program Stunnel pada link di atas, Anda juga harus men-download dua buah file library pendukung yang dibutuhkannya. File tersebut adalah libeay32.dll dan libssl32.dll. Setelah di-download, letakkanlah kedua file ini pada directory yang sama dengan program Stunnel. Dalam contoh ini kami menggunakan directory C:\Program Files\Stunnel. Sampai sini program Stunnel sudah siap digunakan.

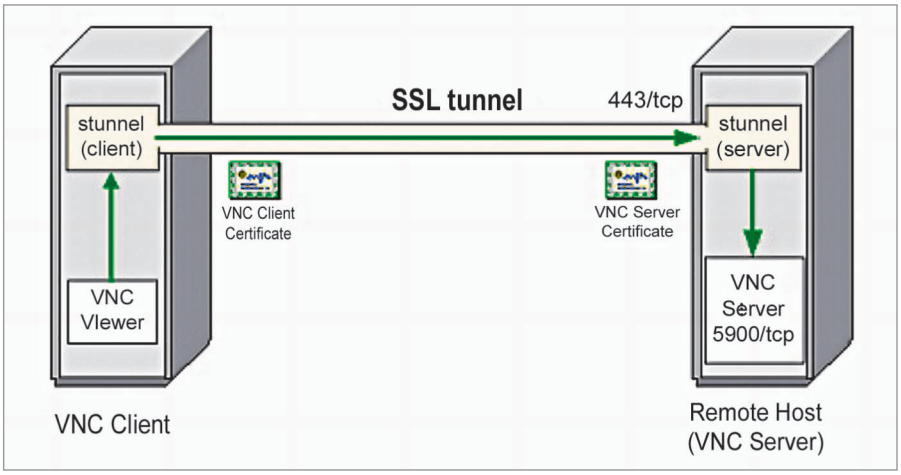
Untuk membuat fasilitas Stunnel ini selalu aktif setiap kali Anda melakukan reboot, Anda harus melakukan sedikit modifikasi pada level registry. Caranya kliklah menu *Start|Run* kemudian ketikkan perintah *Regedit* pada kolom Run setelah itu tekan tombol Enter, maka akan muncul program Registry editor Anda. Bukalah registry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Pada halaman registry tersebut, buatlah registry baru bernama Stunnel dengan jenis REG_SZ. Setelah itu isilah value nya dengan link directory di mana Anda menyimpan program stunnel.

Pada percobaan kami, value-nya kami isi dengan nilai "C:\Program Files\Stunnel\stunnel-4.11.exe". Setelah selesai, program akan berjalan setiap kali Anda reboot.

- **Instalasi OpenSSL**

Pada Linux, Anda tidak perlu repot-repot men-download dan menginstal program ini karena semuanya sudah secara *default* tersedia. Namun untuk Windows, Anda harus menginstalnya lebih dulu. Setelah program di-download, letakanlah program ini pada directory C:\Program Files\OpenSSL agar mudah mengetahuinya. Anda juga harus meletakkan file library libeay32.dll dan libssl32.dll pada folder ini. Selain itu, Anda masih memerlukan dua buah file konfigurasi. File konfigurasi tersebut diberi nama openssl.conf dan ca.bat.

File openssl.conf dapat Anda download di link *http://www.securityfocus.com/data/tools/openssl.conf*. Sedangkan file ca.bat dapat Anda ambil di link *http://www.securityfocus.com/data/tools/ca.bat*. Letakkan kedua file ini pada folder yang sama dengan program utamanya. Setelah semuanya selesai, jika memungkinkan lepaskan dulu perangkat komputer Anda ini dari koneksi jaringan untuk sementara.



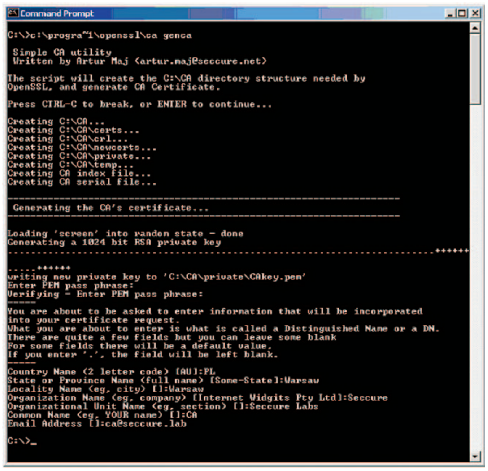
Proses komunikasi client server bukan hanya terjadi di dalam aplikasi VNC saja, tetapi juga di aplikasi Stunnel yang membangun *tunnel* pribadi khusus untuk membawa data VNC.

Konfigurasi Program-program

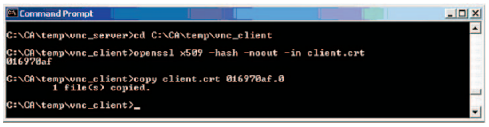
Setelah selesai menginstal, Anda perlu melakukan beberapa konfigurasi untuk menjalankan fasilitas ini.

1. Konfigurasi Certification Authority

Sistem verifikasi sertifikat dengan disertai *public/privat key* merupakan karakteristik dari sistem keamanan SSL



Proses mengenerasi sertifikat otoritas dari PC yang Anda gunakan.



Proses generasi *key* dan sertifikat untuk VNC server.

ini. Untuk itu, Anda perlu membuat semua keperluan itu terlebih dahulu. Langkah pertama, bukalah jendela *command prompt* Anda. Kemudian masuklah ke directory C:\Program Files\OpenSSL. Di dalam directory ini jalankanlah perintah *ca genca*. Ikutilah semua permintaan dari proses ini. Yang terpenting isilah *pass phrase*-nya dengan frase yang cukup sulit ditebak oleh orang lain, seperti halnya password.

Setelah semuanya selesai, Anda akan mendapatkan sebuah directory baru yang berisi file hasil program ini. Directory-nya C:\CA\ dan file CAcert.pem untuk sertifikatnya. Public/Private keynya disimpan dalam file CAkey.pem.

Ulangi langkah di atas, namun dengan mengetikkan perintah *ca server*. Hasilnya adalah file server.key yang merupakan private/public key untuk VNC server, server.crt yang merupakan sertifikat dari VNC server dan file server.pem yang merupakan gabungan file server.key + server.crt (dibutuhkan oleh Stunnel).

Setelah selesai, ulangi sekali lagi langkah di atas, namun kali ini perintah yang diketikkan adalah *ca client*. Setelah selesai prosesnya, maka jadilah file client.key, client.crt, dan client.pem, sama seperti yang terjadi pada proses untuk server. Setelah semuanya selesai, saatnya untuk mengonfigurasikan program Stunnel Anda.

2. Konfigurasi Stunnel

Sebelum dapat membangun koneksi yang aman, program Stunnel harus dikonfigurasikan lebih dulu baik pada sisi VNC server maupun VNC client-nya. Untuk mengonfigurasi program ini, langkah pertama adalah membuat sebuah file bernama stunnel.conf dan harus diletakkan di directory C:\Program Files\Stunnel\stunnel.conf.

File stunnel.conf yang harus diletakkan di VNC server harus Anda isi dengan script seperti di bawah ini:

```
CAfile = CAcert.pem
CApath = certificates
cert = server.pem
client = no
verify = 3
[vnc]
accept = 443
connect = 127.0.0.1:5900
```

Setelah program selesai, *copy*-lah file C:\CA\CAcert.pem dan C:\CA\temp\vnc_server\server.pem ke direktori C:\Program Files\Stunnel. Langkah selanjutnya, ikutilah perintah-perintah ini:

```
cd C:\CA\temp\vnc_client
C:\progra~1\openssl\openssl
x509 -hash -noout -in
client.crt
[Nilai acak hasil perintah
diatas]
copy client.crt [nilai acak
hasil perintah diatas].0
```

Setelah itu letakkanlah file value.0 pada directory C:\Program Files\Stunnel\certificates.

Lakukan hal yang sama untuk program Stunnel yang ada di sisi VNC client. Yang perlu diubah adalah file stunnel.conf menjadi seperti berikut ini:

```
CAfile = CAcert.pem
CApath = certificates
cert = client.pem
client = yes
verify = 3
[vnc]
accept = 127.0.0.1:5900
connect =
VNC_server_IP_address:443
```

Kemudian kopi file C:\CA\CAcert.pem dan C:\CA\temp\vnc_client\client.pem pada VNC client menuju ke direktori C:\Program Files\Stunnel. Dan lakukan juga perintah seperti di bawah ini:

```
cd C:\CA\temp\vnc_server
C:\progra~1\openssl\openssl
x509 -hash -noout -in
server.crt
[nilai acak hasil perintah
diatas]
copy server.crt [nilai acak
hasil perintah diatas].0
```

Setelah selesai simpanlah file [nilai acak hasil perintah diatas].0 ini pada direktori C:\Program Files\Stunnel.

Setelah semua pengaturan yang cukup memusingkan ini selesai, maka solusi ini sudah siap untuk digunakan dengan aman dan nyaman.

Selamat Menikmati Remote Desktop!

Komunikasi *remote desktop* sebenarnya bisa dilakukan dengan banyak cara. Solusi yang ditawarkan kali ini hanyalah satu dari sekian banyak solusi lainnya. Anda bebas memilih dan menikmati komunikasi remote desktop yang Anda suka.

Namun, perlu diingatkan lagi bahwa komunikasi remote desktop tidak dapat digunakan secara sembarangan. Anda harus benar-benar teliti untuk membuatnya karena salah-salah malah dimanfaatkan orang lain atau bahkan PC dan data Anda dirusak oleh orang-orang iseng.

Pilihlah solusi remote desktop yang paling tepat dan nyaman untuk Anda. Setelah itu, selamat menikmati mudahnya bermobilisasi tanpa harus kehilangan desktop PC Anda yang tercinta di kantor atau di rumah. Selamat menikmati! ■

LEBIH LANJUT

- **http://www.wown.com/j_helmig/wxprmdtp.htm**
- **http://www.securityfocus.com/infocus/1677**
- **http://www.microsoft.com/windowsxp/using/mobility/rdfaq.mspx**

Sebuah jaringan komunikasi data yang terawat dengan baik, tentu memiliki sistem monitoring yang baik pula. *Netflow* merupakan sebuah solusi untuk memata-matai isi dari jaringan Anda dengan lebih detail.

Hayri

Netflow, Mata-mata dalam Jaringan

Jaringan komunikasi data Anda tentu harus digunakan sebaik-baiknya. Investasi perangkat switch, router, server, modem, koneksi Internet, dan banyak lagi perangkat jaringan yang tidak murah harganya, tentu harus dibayar dengan efektivitas melakukan pekerjaan. Pekerjaan yang Anda lakukan harusnya dapat lebih cepat terselesaikan dibandingkan dengan sebelum adanya fasilitas jaringan.

Komunikasi antarcabang, antarnegara, antar-*supplier*, antarpelanggan, dan banyak lagi seharusnya dapat dilakukan dengan mudah jika koneksi Internet sudah ada dalam jaringan ini. Jika sudah demikian, maka investasi yang Anda keluarkan tentu akan terbayar dengan cepat.

Namun, apa jadinya ketika jaringan yang seharusnya dilakukan untuk menyelesaikan pekerjaan dengan cepat tidak dapat digunakan untuk melewatkan data Anda. Problem lambatnya koneksi Internet, lambatnya koneksi antar-PC, komunikasi antar-PC yang tidak bisa dibangun, dan banyak lagi problem yang terjadi malah membuat Anda susah untuk bekerja sehingga menghambat pekerjaan yang harus diselesaikan. Tentunya investasi Anda akan sia-sia, bukan? Apalagi ketika jaringan Anda sudah terkoneksi ke Internet, koneksi yang berharga mahal tersebut akan terlewatkan sia-sia.

Jaringan yang tidak bekerja dengan baik memang dapat disebabkan oleh sangat banyak faktor. Saking banyaknya terkadang penyebab problemnya tidak terpikir oleh Anda, padahal terkadang sederhana saja penyebabnya. Bahkan ada beberapa pendapat yang mengategorikan problem di dalam jaringan sering kali berhubungan dengan kekuatan supranatural. Beginilah jadinya jika jaringan Anda tidak dimonitor dengan baik. Pendapat tersebut sama sekali tidak benar.

Untuk dapat menyelesaikan problem dengan cepat dan mudah, Anda sangat memerlukan bantuan sebuah sistem monitoring. Tidak mungkin monitoring jaringan dilakukan secara manual setiap saat. Sebuah sistem monitoring yang baik tentu akan memberikan *report* yang baik dan berguna bagi administrator jaringan tersebut. Report tersebut kemudian akan menjadi bahan analisis Anda yang dapat menjadi kunci bagi misteri problem jaringan Anda.

Sistem monitoring jaringan juga tidak sedikit jumlahnya. Mulai dari sistem monitoring sederhana yang hanya melakukan pengecekkan apakan sebuah perangkat masih aktif atau tidak, pengecekkan volume lalu-lintas data yang melewati sebuah perangkat, hingga yang rumit dan canggih seperti analisis paket-paket data apa saja yang lalu-lalang di dalam sebuah perangkat jaringan, semuanya sudah tersedia dan dapat Anda gunakan sesuai kebutuhan.

Jika Anda membutuhkan sistem monitoring yang cukup canggih untuk mengetahui apa *sih* yang sebenarnya lalu-lalang di dalam jaringan Anda, mengapa tidak coba untuk gunakan fasilitas monitoring jaringan yang cukup canggih yang biasanya tersedia di perangkat jaringan *high end*. Fasilitas monitoring jaringan macam ini disebut dengan nama *netflow*.

Apakah Netflow?

Arti harafiah dari istilah "Flow" adalah sebuah aliran. Aliran yang dimaksud dalam sistem monitoring jaringan

canggih ini adalah aliran data yang keluar dan masuk di dalam sebuah perangkat. Informasi aliran data inilah yang digunakan sebagai bahan analisis yang sangat penting. Sistem penulisan, pengiriman, perhitungan, dan pengaturan informasi yang berupa flow data inilah yang sering disebut dengan istilah sistem netflow.

Sistem perhitungan flow data sebenarnya bukan hanya netflow saja. Protokol Netflow sendiri sebenarnya adalah sistem perhitungan flow yang diciptakan oleh produsen perangkat jaringan terbesar di dunia yaitu Cisco System. Selain netflow, sebenarnya masih banyak protokol penghitung flow lainnya yang biasanya dikhususkan hanya untuk perangkat-perangkat tertentu saja. Hal ini dapat terjadi karena tidak adanya persetujuan resmi untuk menentukan standardisasi dari sistem perhitungan flow ini. Maka dari itu, masing-masing vendor menciptakan sendiri-sendiri untuk perangkat mereka.

Jika di setiap perangkat jaringan bermerk Cisco dilengkapi dengan fasilitas protokol Netflow, di perangkat keluaran Riverstone dan Cabeltron ada sistem perhitungan flow bernama LFAP (*Light-weight Flow Accounting Protocol*). Kemudian ada juga perangkat yang menggunakan sistem sFlow yang sesuai dengan ketentuan RFC3176. Kemudian ada sistem CRANE pada perangkat bermerk XACCT, dan ada lagi beberapa protokol perhitungan flow yang jarang digunakan seperti IPFIX, RTFM, dan IPDR.

Semua sistem dan protokol tersebut bertujuan untuk memberikan laporan dan informasi mengenai apa "isi perut" dari komunikasi yang dilakukan melalui perangkat tersebut. Namun, yang akan banyak dibahas pada artikel kali ini adalah sistem monitoring yang menggunakan netflow. Hal ini dikarenakan pengguna perangkat bermerk Cisco memang mendominasi dunia jaringan komunikasi data saat ini. Jadi mengerti mengenai netflow beserta aplikasi-aplikasinya cukup berguna untuk Anda.

Bagaimana Netflow Dihasilkan oleh Perangkat Jaringan?

Netflow hampir dapat dipasang di semua perangkat jaringan keluaran Cisco yang dilengkapi dengan sebuah processor khusus bernama ASIC. Jadi perangkat yang tidak dilengkapi processor khusus ini belum tentu bisa menghasilkan data flow untuk dianalisis.

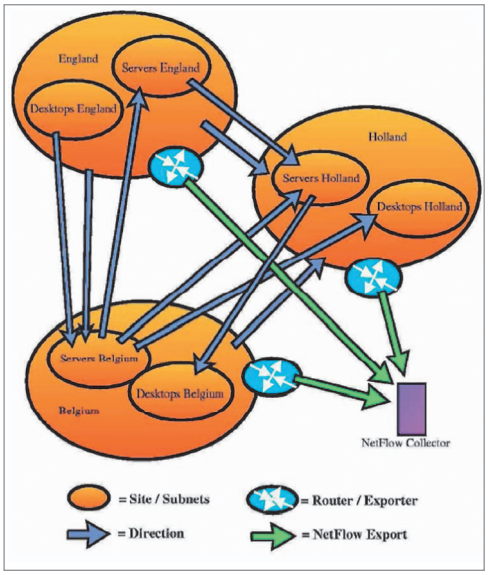
Pada perangkat yang memungkinkan hal itu, Anda tinggal memasang perintah pada interface-intercae yang ingin Anda teliti *traffic*-nya. Perintah tersebut bagaikan sensor, ketika ada data sekecil apapun lewat melaluinya, maka sensor tersebut akan mengetahuinya, menganalisisnya, dan mengubahnya menjadi sebuah informasi statistik tentang karakteristik data tersebut. Informasi yang dimaksud bukanlah isi dari data Anda yang sesungguhnya, melainkan hanya karakteristik dari paket yang membawa data tersebut.

Interface yang dipasangi perintah sensor netflow hanya akan menangkap informasi paket yang masuk (*inbound*) ke dalam interface tersebut. Maksudnya adalah paket-paket data yang datang dari luar dan ingin masuk ke interface tersebutlah yang akan tercatat. Jadi dengan demikian, informasi yang Anda dapat hanyalah paket data apa yang masuk ke sumber tujuan, sedangkan yang keluar tidak pernah tercatat.

Dengan kondisi seperti ini, Anda yang ingin mendapatkan informasi yang lengkap (informasi inbound dan *outbound*) harus mengetahui terlebih dulu paket data Anda keluar dan masuk lewat interface yang mana. Setelah diketahui, pasanglah sensor pada interface-interface tersebut. Jika dipasang pada interface yang tepat, maka Anda akan mendapatkan informasi yang lengkap.

Mengapa Anda Perlu Tahu "Isi Perut" Komunikasi Data dalam Jaringan?

Sistem monitoring yang menggunakan netflow memang sangat berguna bagi para administrasi jaringan. Mereka tidak segan-segan bersusah payah untuk membuat sistem monitoring menggunakan data dari netflow. Mengapa demikian? Karena sistem monitoring jaringan sangat penting untuk dimiliki. Sistem monitoring yang baik adalah sistem yang dapat mengetahui lalulintas data dalam jaringan sedetail-detailnya hingga berakhir pada batas privasi si pemilik data. Selama tidak melanggar privasi dan kerahasiaan data, maka administrator jaringan bebas melakukan monitoring.

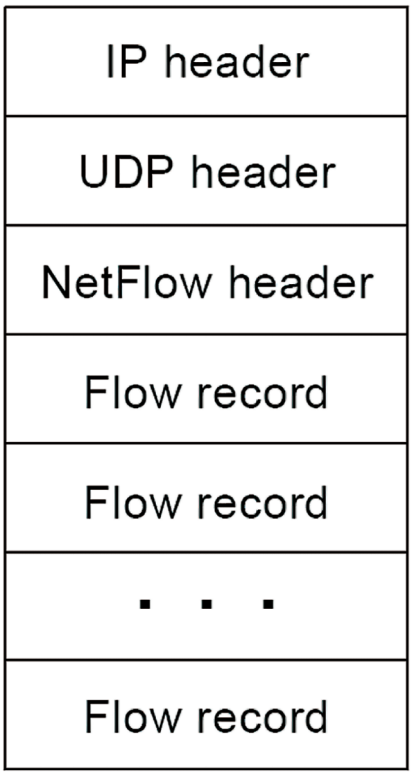


Jika jaringan Anda sudah sebesar ini, maka membutuhkan sebuah server atau perangkat tambahan untuk mengumpulkan semua informasi *flow* dari setiap perangkat.

Dengan menggunakan sistem monitorning menggunakan netflow, maka Anda dapat mengetahui lalu-lintas data dengan lebih detail lagi. Informasi yang detail ini akan sangat berguna sebagai bahan analisis terhadap sifat dan tingkah laku jaringan Anda. Dengan melakukan analisis ini, setiap kejadian, insiden, maupun kegiatan sehari-hari yang berhubungan dengan jaringan dapat terpantau dengan baik tanpa terlewatkan. Baik untuk memonitor penggunaan jaringan dari dalam, serangan-serangan dari luar, virus, program-program terlarang, semuanya bisa dimonitor dengan baik oleh fasilitas ini. Akhirnya informasi ini dapat menjadi bahan pertimbangan dalam mengambil keputusan-keputusan penting.

Informasi Apa yang Dapat Diberikan oleh Protokol Netflow?

Protokol netflow tidak hanya dapat memberikan informasi berapa besar *bandwidth* yang telah terjadi dalam sebuah interface, tetapi jauh lebih banyak daripada itu. Protokol netflow memiliki kemampuan menangkap semua aktivitas yang keluar masuk melalui sebuah interface, kemudian memilah-pilah data tersebut berdasarkan *field-field* informasi yang ada di dalamnya,



Seluruh versi dari *netflow* memiliki jenis *header* yang sama. Yang berbeda hanyalah informasi yang dibawanya keluar dari perangkat jaringan.

dan merepresentasikannya dalam format tabel yang rapi.

Informasi apa yang dibawa oleh protokol netflow bervariasi tergantung pada versi protokol netflow itu sendiri. Namun, informasi yang paling umum dan paling banyak dibutuhkan adalah informasi seputar *Source* dan *Destination* sebuah paket data, jenis port komunikasi apa yang digunakan dalam proses transfernya, waktu pengiriman maupun penerimaannya, *flag-flag* TCP yang ada di dalamnya, dan banyak lagi. Semua data tersebut sangat berguna bagi para administrator jaringan untuk melakukan analisis.

Ada Berapa Versi Protokol Netflow?

Seperti telah dijelaskan di atas, informasi apa saja yang ada di dalam data netflow ditentukan dari versi protokolnya. Versi dari protokol netflow menentukan komponen apa saja yang bisa Anda pakai sebagai bahan analisis terhadap jaringan yang dimonitor. Protokol netflow versi 1 merupakan protokol netflow yang kali pertama keluar. Kurang lengkapnya informasi yang diberikan membuat protokol versi 1 ini sudah tidak direkomendasikan untuk digunakan lagi.

Versi selanjutnya dari protokol netflow adalah versi 5. Dalam versi ini, informasi yang dikirimkan keluar dari perangkat jaringan jauh lebih banyak daripada versi sebelumnya. Informasi yang keluar dari protokol netflow versi 5 adalah sebagai berikut:

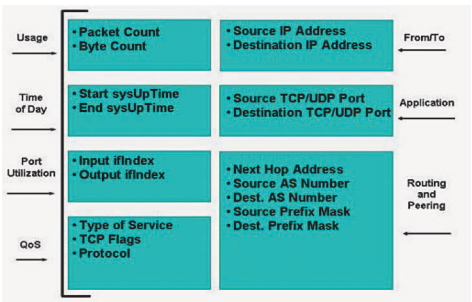
- Source IP address: Alamat asal paket tersebut dikirim.
- Destination IP address: Alamat tujuan ke mana paket tersebut akan dikirim.
- Source TCP/UDP Application port: Port-port aplikasi yang digunakan oleh sumber pengirim data.
- Destination TCP/UDP Application port: Port-port aplikasi tujuan yang akan dituju oleh data.
- Next hop router IP address: Alamat router berikutnya yang akan dituju oleh paket data.
- Input Physical interface index: Nomor index dari interface yang mana data tersebut masuk.
- Output Physical interface index: Nomor index dari interface yang mana data tersebut akan keluar.
- Packet count: Perhitungan flow berdasarkan besarnya paket data.
- Byte count: Perhitungan flow berdasarkan besarnya byte data.
- Start of flow timestamp: Timestamp untuk menandai awal mula flow data terjadi.
- End of flow timestamp: Timestamp untuk menandai berakhirnya flow.
- IP Protocol: Penanda protokol IP apa yang lalu-lalang dalam flow.
- Type of Service byte: Informasi seputar field Type of Service.
- TCP Flags: Informasi seputar TCP flag yang ada dalam sebuah paket.
- Source AS number: Informasi yang menunjukkan dari AS number mana paket data tersebut berasal.
- Destination AS number: Informasi seputar AS number dari mana paket tersebut berasal.
- Source subnet mask: Informasi subnet mask dari alamat IP dari sebuah paket data yang akan keluar.
- Destination subnet mask: Informasi subnet mask dari alamat IP yang dituju oleh sebuah paket.

Netflof versi 5 ini merupakan yang paling umum digunakan, meskipun masih banyak lagi versi yang lainnya seperti versi 7 yang hanya digunakan oleh perangkat switch Cisco, versi 8 yang ditambah fiturnya dengan kemampuan agregasi, dan versi 9 yang diklaim oleh pihak Cisco dapat menyediakan hampir semua informasi penting seputar jaringan mulai dari layer 2 sampai dengan layer 7 dan protokol OSI.

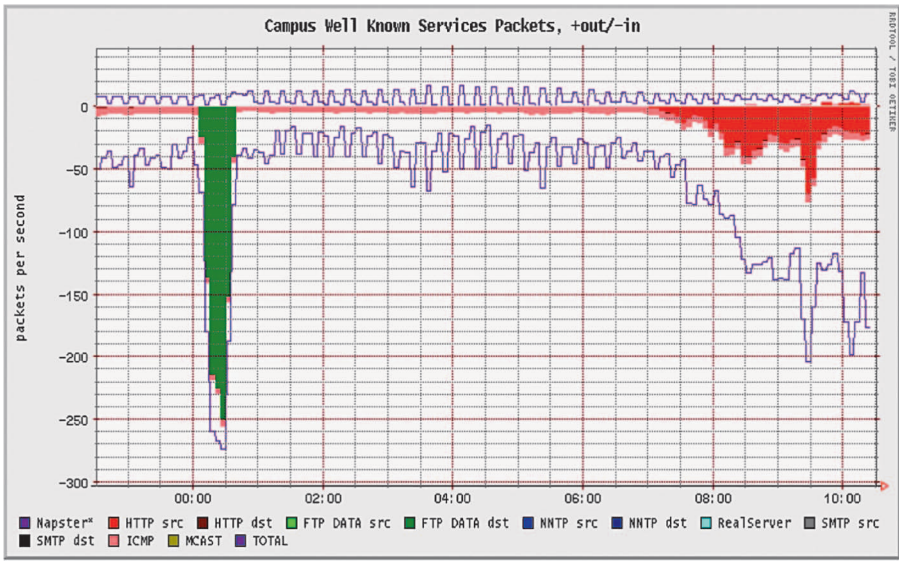
Apakah Fasilitas Netflow Dapat Mengganggu Performa Perangkat Jaringan?

Jika dilihat begitu lengkap dan padatnya informasi yang diberikan oleh netflow, maka Anda mungkin mengiri ini adalah pekerjaan berat buat perangkat jaringan. Namun ternyata pekerjaan itu tidaklah terlalu membebani perangkat jaringan, khususnya produk Cisco. Fasilitas ini menjadi tidak terlalu membebani processor utama dari perangkat dikarenakan fasilitas ini akan dijalankan dengan bantuan ASIC dari perangkat jaringan tersebut. Processor ASIC yang merupakan processor khusus untuk melakukan "pemikiran" pada *level front*, akan memproses semua informasi ini. Karena ASIC jauh lebih spesifik kemampuannya dari processor biasa, maka menjalankan fasilitas netflow menjadi tidaklah membebani.

Menurut sebuah penelitian, sebuah perangkat jaringan yang diberikan informasi flow sebesar 10000 akan menambah penggunaan CPU menjadi sekitar dibawah 4%. Untuk flow yang berjumlah 45000, maka tambahan CPU nya adalah sebesar di bawah 12%. Sedangkan untuk flow sebesar 65000 proses CPU tambahannya adalah sekitar dibawah 16% saja. Dengan demikian, mengaktifkan fasilitas netflow pada



Informasi apa saja yang bisa didapat dari fasilitas *netflow*.



Informasi *traffic* bisa Anda dapatkan secara *realtime* dan juga lebih spesifik karena dapat ditampilkan per servis.

perangkat jaringan tidak terlalu mempengaruhi performanya secara keseluruhan.

Bagaimana Membuat Sistem Netflow?

Membuat sistem yang dapat menangkap, menampilkan, dan menganalisis informasi netflow sebenarnya relatif tidak sulit. Yang Anda butuhkan hanyalah perangkat komputer yang berspesifikasi cukup bagus dan dapat terkoneksi ke jaringan. Dalam membuat sistem netflow, ada tiga komponen penting untuk menjadikannya sebuah informasi yang layak untuk dibaca dan dianalisa oleh manusia. Ketiga komponen tersebut adalah *Netflow collector, Netflow analyzer, Netflow reporter,* dan *Netflow presenter*.

Netflow collector atau secara harafiahnya adalah pengumpul netflow merupakan sistem yang bertugas mengambil dan mengumpulkan informasi netflow yang dikirim dari perangkat jaringan. Informasi yang masih berupa data mentah dikumpulkan dan diubah menjadi sebuah file yang nantinya akan dibaca oleh Netflow analyzer. Netflow analyzer akan membaca data mentah tersebut kemudian menganalisisnya menjadi sebuah bentuk yang dapat dibaca oleh manusia. Setelah diubah bentuknya, maka data netflow tadi dikirim ke Netflow reporter. Di dalam Netflow reporter ini data informasi netflow tadi di pilah-pilah menjadi informasi yang memang Anda inginkan. Anda dapat menentukan informasi apa yang ingin Anda tampilkan di sini.

Netflow reporter kemudian akan mengirimkan ketentuan-ketentuan yang telah Anda buat tersebut ke komponen Netflow presenter. Network presenter inilah yang akan membuat data netflow menjadi grafik, tabel, dan teks yang bisa Anda baca dengan nyaman. Semua informasi terpresentasikan dengan baik dan benar di sini sehingga Anda dapat melakukan analisa lebih lanjut.

Keempat komponen ini harus bekerja sama dengan baik untuk dapat menampilkan informasi dengan baik. Tanpa adanya kerja sama yang baik antara keempat komponen ini atau bahkan salah satunya saja tidak ada, maka Anda tidak akan mendapatkan informasi netflow tersebut.

Aplikasi-aplikasi Pendukung Netflow

Aplikasi-aplikasi pendukung netflow sebenarnya dapat dibagi atas empat komponen penting tersebut. Dalam percobaan, kami menggunakan *operating system* Linux untuk membuat sistem netflow. Dipilih menggunakan Linux karena Anda akan mendapatkan semua program pendukung tersebut tanpa harus membayar sepeser pun dan tanpa harus melakukan kejahatan pembajakan. Mudah dan nyaman, bukan?

Setelah Linux tersedia, kami menggunakan program flow-tools sebagai Netflow collector. Program ini memiliki kemampuan menangkap informasi netflow yang dikirim dari perangkat jaringan dan kemudian meneruskannya kembali ke perangkat lain.

Untuk program Netflow analyzer, kami menggunakan program Flowscan yang sangat mudah dikonfigurasi dan dijalankan. Untuk program Netflow reporter-nya, kami gunakan program JKFlow yang memiliki fasilitas lengkap dalam melakukan filtering data apa saja yang ingin ditampilkan. Setelah semuanya siap, program Netflow presenter-nya kami menggunakan program RRDtool, yang dapat menghantarkan Anda grafik *realtime* yang dipresentasikan dengan sistem *round robin database*.

Semua dinstal dengan mengikuti petunjuk yang diberikan dan dikonfigurasi sesuai keinginan kami. Hasilnya adalah sebuah grafik yang cukup informatif yang ditampilkan oleh komponen dari JKFlow.

Informasi Berguna di Mana-mana

Informasi yang diberikan oleh protokol netflow memang terbilang cukup lengkap untuk sebuah proses analisis. Dari sini Anda dapat mengetahui alamat IP yang dituju, dari mana traffic data berasal, berapa nomor port aplikasi yang digunakan dan ditujunya, serta masih banyak lagi. Ternyata, informasi yang begitu lengkap ini tidak hanya dapat digunakan oleh proses monitoring, namun ada beberapa perangkat yang menggunakan informasi tersebut sebagai bahan pertimbangan pemberian bandwidth, sebagai perangkat intrusion *detection, firewall*, dan banyak lagi. Maka dari itu, monitorlah perangkat Anda mulai sekarang dengan menggunakan netflow. Selamat mencoba! ■

LEBIH LANJUT

- **http://jkflow.sourceforge.net**
- **http://users.telenet.be/jurgen.kobierczynski/jkflow/JKFlow.html**
- **http://users.telenet.be/jurgen.kobierczynski/jkflow/eindwerk.pdf**
- **http://www.dynamicnetworks.us/netflow/**
- **http://netflowguide.com/?page=guide**

Zaman serba digital juga harus diikuti dengan teknologi *storage* yang terus berkembang. *Network storage* merupakan perkembangan dari teknologi storage saat ini. Meskipun sudah cukup lama ada, namun masih tetap menarik untuk dipelajari.

Hayri

Network Storage, Penunjang Kehidupan Digital

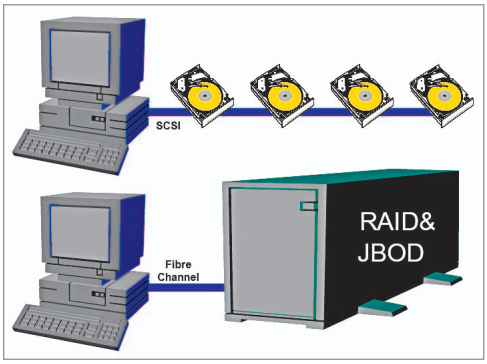
▶Musik jadi MP3, film jadi AVI, lembaran-lembaran dokumen jadi file berekstensi doc, *slide-slide* presentasi jadi file ppt, serta beribu-ribu lembar buku referensi jadi sebuah file berformat pdf. Begitulah kira-kira perkembangan aplikasi teknologi digital dan komputer saat ini. Hampir semua bentuk informasi yang ada di dunia ini dapat diubah menjadi berwujud digital.

Mulai dari bunyi-bunyian musik sampai dokumen bernilai triliunan rupiah kini dapat dengan mudah kita ubah menjadi berbentuk digital. Selain mudah untuk didistribusikan, mudah untuk dirawat, mudah untuk disimpan, data dalam bentuk digital juga lebih kebal terhadap perubahan waktu. Dokumen Anda tidak akan lapuk seperti halnya kertas yang berumur puluhan tahun, atau musik yang mulai mendayu-dayu bunyinya karena pita kaset yang sudah cukup berumur dan sering diputar. Karena sebab-sebab itulah, kini orang lebih memilih untuk menyimpan semua data dan dokumennya dalam wujud digital. Baik untuk kepentingan sederhana, hingga untuk kepentingan bisnis yang besar.

Semakin banyak orang yang menggemari digitalisasi datanya, maka semakin meningkat pula kebutuhan akan media penyimpanannya. Jumlah, besar dan jenis-jenis datanya pun semakin bervariasi seiring dengan berkembangnya aplikasi dan sistem yang menciptakan data tersebut. Perkembangan teknologi komunikasi juga menjadi penyebab berkembangnya jumlah data karena data penting dan besar tidak harus lagi terpusat di suatu tempat, sehingga pengaksesannya lebih mudah.

Perkembangan yang begitu cepat dari informasi digital inilah yang akhirnya mendorong pertumbuhan dari sistem dan media penyimpanan data digital. Kebutuhan akan media penyimpanan menjadi penting untuk diperhatikan ketika Anda akan berhubungan dengan aplikasi penghasil banyak data. Pada akhirnya, aplikasi-aplikasi inilah yang akan mendorong dan menentukan ke arah mana perkembangan sistem dan media storage saat ini dan saat yang akan datang. Sistem storage beserta jenis-jenis medianya menjadi bagian kritikal yang mendapat perhatian lebih dalam melakukan desain sistem.

Untuk itu, ada beberapa faktor yang penting untuk diperhatikan dalam melakukan desain dan implementasi sistem storage dan media penyimpanan pendukungnya. Dengan memperhatikan beberapa faktor ini, sistem storage Anda menjadi bener-benar efektif dalam membantu pekerjaan dan kebutuhan Anda. Faktor-faktor penting tersebut adalah sebagai berikut:



Sistem *storage* sederhana yang ditawarkan oleh DAS memang cocok untuk penggunaan yang sederhana.

- **Capacity**

Karena jumlah data digital kian lama kian meningkat, maka faktor kapasitas menjadi poin yang paling utama dalam memenuhi kebutuhan storage saat ini. Menurut sebuah survai, pertumbuhan kebutuhan kapasitas penyimpanan data pada sebuah perusahaan berkembang melampaui apa yang dinyatakan dalam hukum Moore (perkembangannya melebihi dua kali lipat dalam 18 bulan).

- **Performance**

Performa yang hebat juga harus diperhatikan dalam memilih dan menggunakan sistem *storage* data. Mengapa harus diperhatikan? Karena kecepatan dan kemampuan membaca dari perangkat storage tersebut harus seimbang dengan perkembangan yang terjadi pada perangkat yang menggunakannya. *Bandwidth* untuk menghantarkan data dari media storage harus sesuai dengan kecepatan proses dari komputer yang menggunakannya, harus sesuai dengan performa jaringan komunikasi data yang akan dilewatinya, dan harus sesuai dengan aplikasi yang mengaksesnya seperti misalnya aplikasi multimedia. Maka itu, performa dari sistem storage juga harus diperhatikan benar-benar.

- **Availability**

Karena semakin besarnya ketergantungan masyarakat terhadap data digitalnya, maka ketersediaan dan reliabilitas dari media penyimpanannya juga harus benar-benar diperhatikan dan ditingkatkan. Hal ini menjadi sangat penting untuk menghindari terjadinya kehilangan isi dari data dan kehilangan kesempatan mengakses data yang tersimpan di dalamnya. Maka dari itu, media storage yang memiliki availabilitas dan reliabilitas tinggi sudah barang tentu dibutuhkan untuk mencegah terjadinya kesulitan mengakses data. Selain itu, sistem storage juga harus memiliki sistem penyelamatan data ketika terjadi bencana, seperti misalnya memiliki sistem *mirroring* atau teknik *back-up* yang dapat meng-*copy* data yang disimpannya ke lokasi-lokasi yang berbeda.

- **Scalability**

Solusi penyimpanan data yang telah Anda miliki idealnya tidak hanya dapat memenuhi kebutuhan saat ini saja, melainkan dapat juga mengatasi perkembangan kebutuhan di masa yang akan datang. Sistem penyimpanan ini hendaknya dapat berkembang dengan mudah seiring dengan berkembangnya kebutuhan akan penyimpanan.

- **Cost**

Media storage yang tentu dipasang dalam kapasitas yang sangat besar hendaknya harus juga memiliki harga yang tidak terlalu memberatkan penggunanya. Hal ini dikarenakan pengguna pasti akan terus membutuhkan media penyimpanan selama datanya masih ingin disimpan, maka itu dengan harga media penyimpanan yang murah, pengguna tidak akan lepas dari penggunaan media tersebut. Harga sistem penyimpanan yang murah sebaiknya bukan hanya dari segi perangkat kerasnya saja, namun juga termasuk murah dalam *maintenance* dan manajemen dari sistem storage tersebut.

Dengan didorong oleh faktor-faktor di atas, bermunculanlah perkembangan teknologi sistem storage yang bertujuan untuk memenuhi semua kebutuhan tersebut. Teknologi networking pun akhirnya diadopsi untuk disulap menjadi sebuah sistem storage yang mampu melayani penyimpanan data dalam skala enterprise. Dalam artikel ini, akan banyak dibahas mengenai beberapa model dan teknologi penyimpanan data yang berada di dalam jaringan dan bahkan mengadopsi teknologi jaringan untuk mendukung kinerjanya.

Apa Saja Model dan Teknologi Storage?

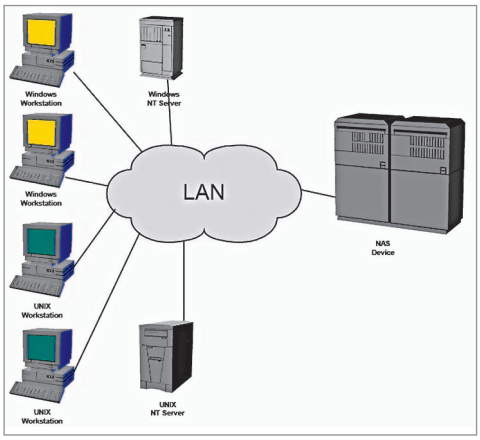
Teknologi *storage* memang terus berkembang seiring dengan perkembangan kehidupan digital. Dari perkembangan ini, saat ini tersedia tiga jenis model teknologi data storage yang banyak digunakan. Teknologi tersebut adalah *Direct Attached Storage* (DAS), *Network Attached Storage* (NAS), dan *Storage Area Network* (SAN).

Terlepas dari siapa yang terbaik, semua sistem ini memiliki kegunaan dan keunggulannya masing-masing untuk memenuhi kebutuhan Anda. Teknologi-teknologi ini akan mendukung kebutuhan Anda dalam skema aplikasi dan lingkungan yang berbeda-beda.

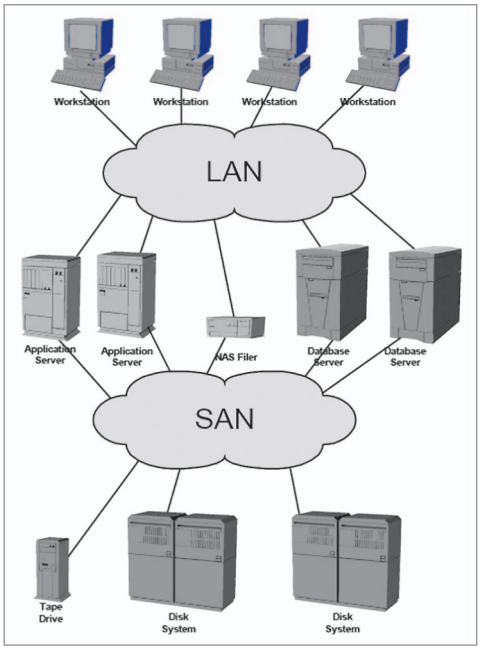
Apakah Direct Attached Storage?

Sistem DAS ini merupakan teknologi yang paling sederhana dan paling umum digunakan di dalam berbagai kehidupan digital Anda. Sistem DAS ini akan banyak ditemukan didalam server-server, *standalone* PC, *workstation*, dan banyak lagi. Konfigurasi DAS yang umumnya terjadi adalah terdiri dari sebuah komputer yang terkoneksi secara langsung dengan satu atau lebih harddisk penyimpan data atau *disk array*. Dengan kata lain, PC atau perangkat komputer Anda langsung dipasangi satu atau lebih harddisk yang dapat diakses secara langsung untuk menyimpan dan membuka data Anda.

Jalur komunikasi yang digunakan antara PC dengan media penyimpanan ini adalah menggunakan sistem standar



Sekumpulan media penyimpanan yang tergabung kedalam jaringan dan dapat melakukan transaksi di dalamnya merupakan fasilitas yang sangat membantu. Ini ditawarkan oleh teknologi *storage* NAS.



Dengan menggunakan area yang terpisah, SAN menjadi sangat hebat performanya.

bus yang biasa digunakan untuk mengoneksikan antara harddisk dengan sistem komputer Anda, seperti misalnya SCSI, ATA, Serial ATA (SATA), dan Fiber Channel (FC).

Beberapa dari sistem *cabling bus* yang telah disebutkan di atas, memungkinkan untuk melakukan penyatuan beberapa harddisk menjadi satu. Yang paling umum digunakan dalam praktik sehari-hari di PC atau server sederhana Anda adalah menyatukan beberapa buah harddisk SCSI dengan *interface* dan sistem bus SCSI. Sistem sederhana seperti ini sudah dapat dikategorikan sebagai sistem DAS sederhana.

Contoh penggunaan lainnya adalah mengoneksikan PC atau server Anda ke sebuah perangkat media penyimpanan yang isinya terdiri dari banyak harddisk dengan menggunakan koneksi Fiber Channel. Di dalam perangkat media penyimpanan tersebut berisikan harddisk array yang dibuat menjadi satu kesatuan dengan sistem RAID, atau hanya sekumpulan harddisk biasa saja yang tidak disatukan. Sistem seperti ini juga termasuk dalam kategori DAS.

Penggunaan DAS dalam jaringan skala besar sangatlah luas. Sistem storage ini relatif cukup mudah untuk dimengerti, diinstalasikan dan dijalankan. Sistem storage ini juga relatif tidak mahal untuk dimiliki. DAS sangat cocok digunakan untuk kebutuhan sederhana yang tidak mementingkan penambahan kapasitas yang sangat banyak jika suatu saat dibutuhkan, tidak memerlukan administrasi yang rapi, tidak membutuhkan mekanisme *back-up* otomatis, performa, dan tingkat availabilitas yang tinggi. Dengan kata lain, DAS merupakan solusi sistem storage kelas *low end* atau kelas *individual storage*.

Sistem storage DAS ini sangat dan memang harus terikat pada PC atau perangkat komputer individual untuk dapat digunakan. Dengan demikian, DAS juga akan bergantung kepada sistem operasi dan performa dari PC yang membawahinya. Dengan demikian, DAS memiliki semua kelemahan yang ada pada PC tersebut. Performa dari sistem storage ini akan sangat bergantung kepada kecepatan proses yang dapat dilakukan oleh PC di atasnya. Jika lambat, maka sistem storage ini juga melambat. Jika PC atau server mati total, maka sistem ini pun tidak akan bekerja.

Sistem DAS juga bergantung kepada berapa banyakkah harddisk yang dapat dilayani oleh sistem bus yang ada pada PC tersebut. Penambahan dan pengurangan harddisk akan sangat berpengaruh terhadap performa keseluruhannya, sehingga *downtime* sistem storage ini mungkin saja terjadi.

Probabilitas data hilang juga cukup tinggi di dalam sistem DAS karena tidak ada sistem back-up yang pasti, kecuali dari PC yang berada di atasnya. Jika sistem back-up memang diaktifkan pada PC tersebut, maka jadilah back-up. Jika tidak, maka data Anda akan berada di ujung tanduk. Performa dalam melakukan back-up juga sangat bergantung kepada PC di atasnya. Interaksi manusia juga masih sangat dibutuhkan di sini. Jika terjadi kelalaian sedikit saja, maka data Anda tidak akan selamat.

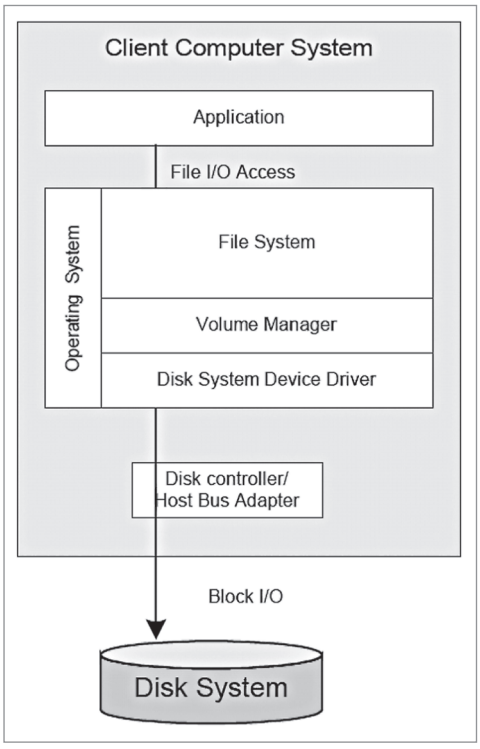
Apakah Network Attached Storage (NAS)?

Setelah melihat bagaimana sistem storage DAS memiliki begitu banyak kelemahan dalam memberikan layanan pada pengguna kelas *enterprise*, maka solusi untuk kebutuhan tersebut adalah dengan membuat sistem storage yang lebih terbuka untuk umum dan lebih pintar dalam mengatur transaksi data yang keluar-masuk darinya. Untuk kebutuhan itu, sistem storage NAS dan SAN merupakan jawabannya.

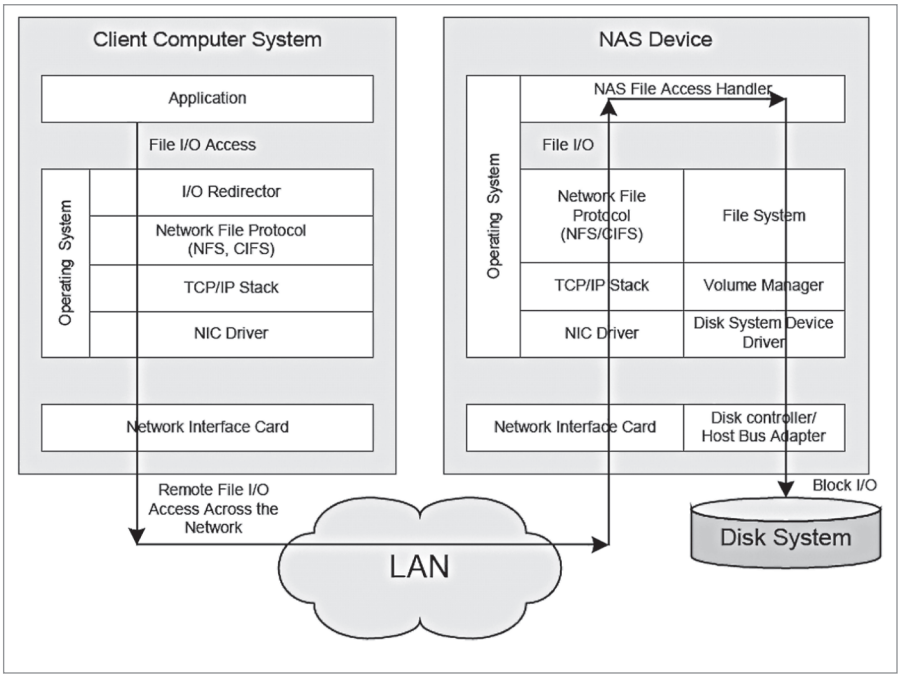
Keduanya memiliki persamaan, yaitu dapat melayani penggunanya dengan menggabungkan diri ke dalam jaringan. Semua pengguna yang tergabung dalam jaringan tersebut bisa mengakses sumber datanya jika menggunakan kedua sistem storage ini. Namun, yang membedakan kedua jenis storage sistem ini adalah cara kerjanya.

NAS secara umum dapat diartikan sebagai sekelompok media penyimpanan yang secara langsung terkoneksi ke dalam jaringan lokal (LAN) dengan menggunakan file sistem khusus jaringan seperti NFS dan CIFS. Perbedaan yang mencolok antara NAS dengan SAN adalah NAS melakukan semua transaksi keluar masuk data dalam jaringan pada tingkatan file-*level*, sedangkan SAN melakukannya pada tingkatan *block-level*.

Transaksi file-level maksudnya adalah NAS melakukan pembacaan permintaan



Cara kerja dari sistem *storage* DAS masih sangat bergantung kepada spesifikasi komputer *client* yang ditumpanginya.



NAS memang cukup membantu Anda dalam melakukan penampungan dalam skala besar.

dan kemudian melakukan transaksi data dalam bentuk file yang sudah jadi dan siap dibaca oleh perangkat komputer yang memintanya. Semua permintaan dan perintah yang berhubungan dengan data di dalamnya diterjemahkan lebih dulu oleh perangkat NAS menjadi sebuah perintah yang menjalankan transaksi dalam tingkatan file level. Setelah perintah diterima perangkat NAS, proses penterjemahan terjadi di dalamnya.

Dari perintah pada tingkat file level diterjemahkan menjadi perintah block level untuk mengakses data di dalam harddisk-nya. Ini berarti penambahan lapisan kerja baru untuk transaksi data ini. Proses penerjemahan ini tentu memakan cukup banyak sumber daya, terutama processor dan waktu proses. Inilah yang merupakan perbedaan utama antara NAS dengan SAN sekaligus menjadi kelemahan untuk NAS. Proses yang dibutuhkannya membuat sumber-sumber daya terpakai maksimal, sehingga proses lain menjadi terganggu. Waktu menunggu pun menjadi lebih lama karena proses penterjemahan membutuhkan waktu yang cukup lama jika dilakukan dengan data yang berukuran besar.

Keuntungan yang Anda dapat dari sistem storage NAS ini adalah kemudahan penggunaannya yang relatif cukup sederhana. Banyak *operating system* yang sudah mendukung proses komunikasi dengan protokol file sistem NAS seperti misalnya NFS dan CIFS. Sistem operasi Linux dan UNIX telah lama mendukungnya, sedangkan Windows versi terbaru pun juga sudah mendukungnya.

Untuk menggunakan NAS Anda tinggal melakukan pengaturan perangkat NAS, mengoneksikannya ke dalam jaringan LAN, kemudian mengonfigurasi sistem operasi pada PC-PC di dalam LAN tersebut untuk dapat berkomunikasi dengan file sistem NAS. Orientasinya pada file level sangat cocok untuk diterapkan pada jaringan yang heterogen yang terdiri dari bermacam-macam sistem di dalamnya. Implementasi NAS juga tidak membutuhkan banyak perubahan pada desain jaringan yang telah berjalan.

Apakah Storage Area Network (SAN)?

Dari segi teknologi, SAN tidak banyak yang berbeda dengan NAS. Hanya saja, yang menjadi perbedaan utama dan yang paling menonjol adalah perbedaan mekanisme transfer datanya. Mekanisme transfer data dari perangkat komputer penggunanya menuju ke media penyimpanan dalam sistem SAN tidak dilakukan dalam tingkatan file-level melainkan dalam tingkat block level.

SAN biasanya menggunakan Fiber channel atau ethernet (iSCSI) sebagai koneksi antara perangkat pengguna dengan media penyimpanannya karena secara fisik perangkat komputer dengan media penyimpanannya kini sudah menjadi bagian yang terpisah. Kini keduanya memiliki hubungan sebagai "peer" yang dapat saling berkomunikasi dengan bebas dengan siapapun. Keuntungan adanya sistem seperti ini adalah media penyimpanan jadi dapat digunakan oleh siapa saja, data didalamnya bisa diakses oleh banyak orang, dan dengan sistem SAN yang rapi maka media penyimpanan ini memiliki tingkat availabilitas yang tinggi.

Sistem storage SAN biasanya berada dalam segmen jaringan yang terpisah dengan LAN yang sehari-hari digunakan. Hal ini bertujuan untuk mengurangi interferensi dengan komunikasi-komunikasi lainnya dalam jaringan lokal, sehingga proses transfer data apalagi blok data yang sensitif terhadap latensi tidak terganggu. Karakteristik sistem seperti ini sangat berguna bagi perusahaan besar yang mengandalkan pemrosesan data digital dalam jumlah yang sangat besar. Dengan mengonsentrasikan penyimpanan data pada sebuah area khusus dan didukung media komunikasi yang cepat, data besar Anda tidak lagi jadi masalah untuk disimpan maupun diakses.

Pilih Solusi yang Tepat

Kebutuhan sistem storage saat ini memang tidak bisa ditunda-tunda. Semakin mekarnya kehidupan digital, semakin penting teknologi sistem storage beserta media penyimpanannya untuk diperhatikan. Perkembangan teknologi storage masih akan terus berlanjut, tidak hanya terbatas pada ketiga sistem ini saja. Aplikasinya pun akan semakin bermacam-macam. Maka dari itu, jika Anda memang sangat membutuhkan media penyimpanan beserta sistem storage-nya, hati-hatilah dalam memilih. Pilih sistem network storage yang sesuai dengan karakteristik penggunaan dan kebutuhan Anda. Selamat belajar! ■

LEBIH LANJUT

- **www.serverworldmagazine.com/webpapers/2000/03_mti.shtml**

Dalam perkenalan ke editor teks Emacs, kita akan mengungkap *shortcut* yang ada dan bagaimana cara menguasai mereka.

Gunung Sarjono

Editor Teks pada Linux

▶*Operating system* mana yang Anda gunakan? Ini merupakan pertanyaan yang sulit, tetapi karena kita sedang dalam konteks Linux maka kemungkinan besar Anda menjawab "Linux", atau mungkin dalam istilah Free Software Stallman Anda menjawab "GNU/Linux". Namun, kali kini kita akan melihat aplikasi terbesar pada semua Linux. Ini merupakan program dikatakan orang sebagai operating system sejak bertahun-tahun yang lalu. Ya, kita berbicara tentang Emacs.

Lebih Baik dengan Meta

Emacs merupakan editor teks pilihan *hacker* elit, sebagian karena Emacs begitu fleksibel sehingga Anda benar-benar bisa menghabiskan seluruh jam kerja tanpa ke luar darinya, tetapi juga karena butuh waktu belajar yang tinggi sehingga Anda bisa saja membanggakan diri kepada yang lain. Untuk menjalankan, ketik 'emacs' dari terminal Anda. Jika Anda menjalankan X, ini otomatis akan membuka versi grafis dari Emacs, yang memungkinkan Anda menggunakan mouse untuk kontrol ekstra. Jika Anda tidak menjalankan X, ini akan membuka versi terminal dari Emacs; Anda juga bisa membuka versi terminal dari dalam X dengan menjalankan 'emacs -nw'. Kami sarankan untuk mengunakan versi grafis sampai Anda bisa berdiri sendiri, di mana pada saat itu Anda bisa memilih mana yang terbaik untuk Anda.

Emacs menggunakan *shortcut* keyboard yang luas, tetapi Anda juga bisa bekerja dengan mouse. Contoh tombol kontrol adalah [Ctrl] dan [Alt] (biasanya disebut sebagai 'Meta'). Sebagai contoh, menekan 'Ctrl-x' kemudian 'Ctrl-c' adalah perintah untuk keluar Emacs—Anda harus menekan dan menahan 'Control', kemudian tekan 'X', kemudian tekan 'C'. Menggunakan dua tombol secara bersamaan seperti ini disebut shortcut 'chord' dan ini sering kali digunakan pada Emacs—sangat sering malah. Tombol [Ctrl] dan 'Meta' tersebut biasanya disebut 'C' dan 'M' saja, jadi shortcut untuk keluar adalah 'C-x C-c'.

Shortcut penting lain untuk membantu Anda adalah 'C-x C-f' untuk memuat file, dan 'C-x C-s' untuk menyimpan file. Pada keduanya, Anda akan diminta untuk mengetikkan nama file di bagian bawah layar. Pada waktu membuka beberapa file, Anda bisa berpindah antara mereka dengan menggunakan menu *Buffers*. Disebut demikian karena setelah file dibuka mereka disebut sebagai 'buffers'. Cara lain, Anda bisa mengetik 'C-x b' (yaitu, tekan dan tahan [Ctrl], tekan 'X', kemudian lepas kedua tombol dan tekan 'B'), kemudian ketik nama file yang ingin Anda tuju (tanpa path). Emacs akan mem-*prompt* Anda dengan opsi *default*, yang biasanya buffer sebelumnya yang Anda lihat—tekan [Enter] untuk menggunakan default-nya. Setelah file terbuka, Anda bisa mengetik seperti biasa untuk mengedit teks, kemudian simpan dengan 'C-x C-s'.

Search dan Replace

Perintah dasar untuk *search* dan *replace* pada Emacs dilakukan dengan 'C-s', dan kemudian ketik yang ingin Anda cari. Pencarian hanya dilakukan ke depan. Untuk mencari ke belakang, gunakan 'C-r'. Untuk mengulangi pencarian, cukup ketik perintah dua kali, yaitu 'C-s C-s' atau 'C-r C-r'. Itu merupakan bagian yang mudah, tetapi *search* dan *replace* memerlukan tombol *Meta*.

Untuk menjalankan perintah replace sederhana, tekan 'M-x' (tahan [Alt] kemudian tekan 'X'), ketik 'replace-string' dan tekan [Enter]. Emacs akan menanyakan Anda string yang ingin dicari (tekan [Enter] lagi setelah mengetikkannya), kemudian ia akan menanyakan string yang digunakan sebagai pengganti (sekali lagi, tekan [Enter] setelah Anda mengetikkannya). Ini menjalankan 'replace all' search, tanpa input lebih lanjut dari Anda. Jika Anda ingin kontrol lebih, coba 'M-x query-replace', yang meminta Anda memasukkan string yang dicari dan string pengganti seperti sebelumnya, tetapi kemudian meminta konfirmasi Anda untuk setiap perubahan yang ditemukan—tekan 'y' untuk menerima perubahan, atau 'n' untuk menolak.

Jika sudah merasa mahir, Anda bisa menggunakan shortcut untuk shortcut (apakah Anda lihat mengapa Emacs sulit sekali sekarang?), dengan mengetik 'M-%' utuk menjalankan *query replace*. Pada praktiknya, tanda '%' didapat dengan menekan [Shift] dan menekan '5', jadi Anda harus menahan [Alt], menahan [Shift] dan menekan '5'. Jika ada perubahan dalam *search* dan *replace*, Anda bisa membatalkan tindakan terakhir dengan 'C-x u'. Suatu 'tindakan' adalah satu perubahan lengkap, yang artinya satu perubahan jika Anda menggunakan 'query-replace', atau banyak perubahan jika Anda menggunakan 'replace-string'. Cara lain, ada item *Undo* di bawah menu *Edit*, bersama dengan beragam item search dan replace, yang artinya Anda tidak perlu terlalu khawatir mengenai shortcut jika Anda tidak benar-benar menginginkannya!

Cut, Copy, dan Paste

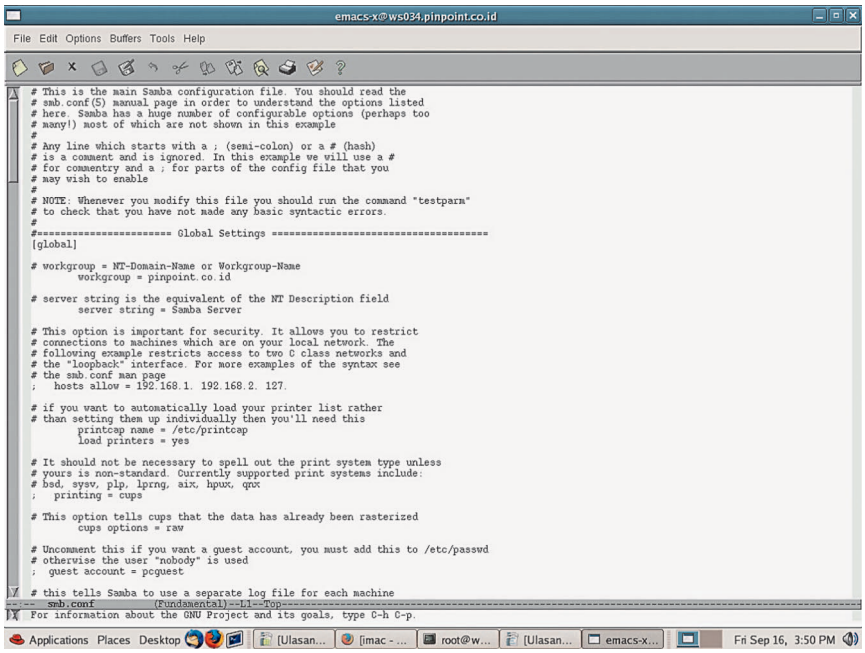
Karena kita sekarang sedang menggunakan versi grafis, ketiga operasi ini bisa dilakukan dengan menggunakan

EMACS: DI BELAKANG LAYAR

■ Pada waktu kami menyebutkan bahwa Emacs dianggap sebagai suatu OS oleh kebanyakan orang, kami sungguh-sungguh. Dengan memandang sekilas beberapa item menu, tentu telah menunjukkan seberapa banyak di situ yang ditawarkan. Fleksibilitas Emacs bisa dilakukan karena ia mempunyai bahasa pemrograman Lisp yang dimasukkan ke dalamnya, sehingga orang-orang bebas membuat *add-on* yang sangat kompleks untuknya.

Sebagai contoh, di bawah menu *Tools* Anda akan melihat kontrol untuk membaca Usenet dan e-mail, menjalankan *patch* dan membandingkan file, menjalankan *debugger* dan memainkan *game*. Game yang ada sangat sederhana—Snake, Tetris, dan Adventure (RPG berbasis teks) adalah di antaranya. Namun, mungkin yang paling menarik dari semuanya adalah Emacs psychiatrist, yang berada di bawah menu Help. Di situ Anda bisa mengeluarkan emosi, mengurangi rasa takut, dan nyatakan keyakinan Anda sementara dokter Emacs seolah-olah mendengarkan Anda. Hanya saja jangan berharap terlalu banyak! Yang jauh lebih menarik adalah menekan 'M-x' kemudian menjalankan psychoanalyze-pinhead, yang menggunakan kutipan dari Zippy the Pinhead input untuk psychiatrist Emacs—tekan 'C-c' untuk berhenti.

Emacs mempunyai sesuatu untuk semua orang. Sebagai contoh, jika



Anda menghabiskan beberapa tahun dari kehidupan Linux Anda untuk mempelajari editor Vim, Anda bisa mentransfer pembelajaran ke Emacs melalui 'Viper' mode. 'Viper' merupakan singkatan dari '*Viper is a Package for Emacs Rebel*', sehingga jelas bahwa meskipin pengguna Vim dan Emacs sangat berbeda dalam memilih editor, paling tidak ada yang bisa diambil.

Ketik 'M-x viper-mode' untuk meng-*enable* Viper mode. Emacs akan menanyakan apakah Anda ingin mematikan pesan *start-up* (ketik 'no' supaya Anda bisa setiap kali melihat layar info), kemudian Viper akan menanyakan Anda mengenai 'Viper level'. Secara sederhana, Viper level 1 bekerja hampir sama dengan Vim, level 2 menambahkan beberapa fitur Emac, level 3 menambahkan lebih banyak lagi, level 4 mulai terasa seperti setengah Emacs, dan level 5 merupakan campuran Vim dan Emacs. Mulailah dengan level 1. Kami sarankan untuk tidak membuat perubahan permanen, supaya Anda bisa dengan mudah memilih level lain sesuai peningkatan kompetensi Anda. Setelah dalam Viper mode, tekan 'Escape', kemudian tekan ':q' untuk berhenti, begitu juga dengan Vim.

VIM: TEMPAT ANDA BERPALING

Keuntungan Emacs adalah Anda tidak perlu meninggalkan arenanya yang luas. Ia menggabungkan editor teks dengan *debuggger, psychiatrist, change viewer*, dan *mail reader*. Namun, tidak semua orang menginginkan itu. Banyak orang ingin editor teks mereka berfungsi sebagai editor teks saja, dan menyerahkan semua yang lain ke program yang bisa melakukan mereka lebih baik. Bagi orang seperti ini—dan sejujurnya mereka mayoritas—Vim merupakan pilihan yang paling populer.

Vim merupakan singkatan dari *Vi Improved* karena lebih maju dari Vi, yang merupakan editor Unix klasik yang dibuat oleh **Bill Joy** dan kawan-kawan pada pertengahan 1970-an. Ia menelan Emacs selama beberapa tahun, dan ini segera tampak karena Vim kurang begitu kompleks. Bahkan Vim, yang memasukkan banyak fitur, masih jauh lebih kecil dan sederhana dibanding Emacs. Berkebalikan dengan umur Vim, Anda akan selalu menemukannya (atau Vi) terinstalasi pada hampir semua mesin Unix yang Anda jumpai. Untuk menjalankannya, ketik 'vi' pada command line. Kebanyakan distro Linux menghubungkannya ke Vim, jadi Anda bisa langsung menggunakannya. Jika Anda belum mempunyai Vim, bisa diinstalasi dari *package manager*.

Perintah Dasar

Setelah berada dalam Vim, Anda bisa navigasi dengan menggunakan tombol kursor. Secara resmi, cara yang benar adalah dengan menggunakan tombol H, J, K, dan L untuk bergerak ke kiri, bawah, atas, dan kanan. Programer mengklaim bahwa cara ini lebih cepat, tetapi Anda boleh saja menggunakan kursor kecuali jika Anda terkoneksi dari remote terminal yang tidak menangani mereka dengan baik. Pada waktu kali pertama menjalankan Vim, Anda akan berada dalam Normal mode, yaitu Anda bisa navigasi dengan kursor dan menjalankan perintah. Jika ingin keluar dari Vim, tekan ':q'. Ini akan menghentikan Vim dan mengembalikan Anda ke *command line*.

Untuk kembali ke Vim, ketik 'vim myfile.txt' supaya langsung membuka file myfile.txt untuk diedit. Jika file tidak ada, Vim akan membuatkannya untuk Anda. Sekarang, tekan 'i' untuk memasuki Insert mode—ini memungkinkan Anda untuk memasukkan teks, jadi silakan mengetik dengan bebas. Setelah selesai, tekan [Esc] untuk kembali ke Normal mode, dan Anda akan bisa melakukan navigasi lagi dengan menggunakan tombol kursor. Untuk menghapus suatu huruf, pindahkah kursor ke huruf tersebut, kemudian tekan Delete (bukan Backspace) untuk menghilangkannya. Jika Anda coba keluar dari Vim sekarang, Anda akan melihat Vim menampilkan peringatan bahwa file telah diubah. Anda harus memberitahu untuk menulis atau berhenti tanpa menyimpan.

Untuk menulis suatu file, jalankan perintah ':w'. Untuk keluar tanpa menyimpan, ketik ':q!'. Cara lain, jika Anda ingin menulis kemudian berhenti, gunakan ':wq'. Seperti yang Anda lihat, Anda bisa menggabungkan dua perintah bersama-sama. Selagi dalam Vim, Anda bisa membatalkan perintah terakhir dengan menekan 'u'. Vim menyimpan jejak undo yang panjang jadi Anda bisa membatalkan beberapa perubahan dengan menekan tombol beberapa kali. Ada juga beberapa perintah navigasi tambahan. *Page Up* dan *Page Down* bekerja seperti biasa, tetapi Anda juga bisa menggunakan '$' (pindah ke akhir baris), '^' (ke awal baris), 'w' (ke awal kata berikutnya), dan 'e' (ke akhir kata berikutnya).

Mengubah Teks

Sama seperti menulis dan berhenti, Anda bisa meggunakan perintah navigasi tambahan bersama dengan perintah lain. Sebagai contoh, perintah 'delete' Vim adalah 'd'. Anda bisa menggunakannya dua kali untuk menghapus baris. Namun, Anda bisa menggunakan 'd$' untuk menghapus dari posisi kursor saat itu sampai akhir baris, atau 'dw' untuk menghapus kata itu saja.

Ini bahkan semakin *powerful* pada waktu Anda memasukkan angka. Sebagai contoh, 'dd' menghapus satu baris, tetapi '5dd' menghapus lima baris, '500dd' menghapus 500 baris, dan '5dw' menghapus lima kata berikutnya. Anda juga bisa menggunakan angka plus tombol kursor. Misalnya, '5 | Up' pindah lima baris ke atas. Cara cepat untuk mengingatnya adalah pertama Anda tentukan angkanya, lalu tindakannya, kemudian objek dari tindakan, jadi '5dw' menunjukkan angka 5, tindakan-

mouse. Sama seperti editor teks yang lain, Anda bisa memilih teks dan kemudian gunakan *Cut, Copy*, atau *Paste* dari menu *Edit*. Tentu saja, jika ingin mempelajari Emacs dengan benar, Anda harus mempelajari *shortcut*. Ini lebih kompleks ketika Emacs bekerja dalam *console* karena Anda harus bisa memilih teks tanpa mouse.

Hal pertama yang perlu dilakukan adalah meletakkan kursor di mana Anda ingin mulai meng-copy. Sekarang tekan 'C-spasi', spasi adalah Spacebar pada keyboard. Sekarang pada waktu memindahkan kursor, teks akan disorot dalam warna biru yang menunjukkan pilihan Anda. Setelah mendapatkan teks yang diinginkan, tekan 'M-w' untuk meng-copy teks ke clipboard (jadi Anda meng-copy, kemudian menghapusnya). Sekarang pindahkan kursor ke mana Anda ingin mem-paste, dan tekan 'C-y' (yang merupakan singkatan dari *yank*) untuk *paste*. Kata 'yank berarti 'paste' pada Emacs, tetapi 'copy' pada Vim.

File Help

File help untuk Emacs dimasukkan ke dalam editor dan Anda bisa mengaksesnya, baik melalui menu atau melalui shortcut. Untungnya, bagi sebagian besar dari kita, file help secara seragam terdiri dari shortcut 'C-h' dan tombol lain. Jika Anda menginstalasinya, tempat terbaik untuk mulai adailah Emacs tutorial ('C-h-t). Di situ terdapat banyak contoh teks untuk memasukkan diri Anda ke dalam alur berpikir Emacs. Jika Anda sudah bekerja dengan lancar, Emacs FAQ ('C-h F') akan

nya ‘delete’, dan objek yang di-*delete* adalah ‘word’.

Bersama dengan ‘i’ untuk Insert mode, Anda bisa menggunakan ‘a’ untuk Append mode, yang secara garis besar melakukan hal yang sama. Namun, ‘A’ (huruf besar), memasukkan Anda ke dalam Append mode dan memindahkan kursor ke akhir baris. Anda juga bisa menggunakan ‘R’ (huruf besar) untuk memasuki Replace mode, yang menimpa teks pada waktu Anda mengetik. Gunakan [Esc] untuk kembali ke Normal mode.

Jika Anda menggunakan ‘:w’ saja, Vim akan menyimpan file dengan nama yang sama. Anda bisa menggantinya dengan menggunakan ‘:w somefile.txt’, atau juga ‘:wq somefile.txt’, jika Anda ingin langsung keluar. Untuk meng-copy teks ke clipboard, gunakan ‘yy’. Ini akan meng-copy baris saat itu, tetapi Anda juga bisa menggunakan ‘2yy’ untuk meng-copy baris saat itu dan berikutnya, atau ‘100yy’ untuk meng-copy baris saat itu dan 99 berikutnya. Untuk *paste*, gunakan ‘p’, atau ‘10p’ untuk paste sepuluh kali.

Search dan Replace

Search dan *replace* pada Vim menggunakan ekspresi Unix biasa yang tidak asing lagi bagi programer Perl, meskipun tidak terbukti terlalu menyulitkan bagi para pemula. Untuk mencari, ketik ‘/’ kemudian kriteria Anda, dan tekan [Enter]. Secara *default* semua yang cocok akan disorot, dan memindahkan kursor ke yang pertama. Untuk pindah ke yang cocok berikutnya ketik ‘/’ dan tekan [Enter]. Untuk melakukan pencarian ke belakang gunakan tanda tanya, misalnya: ‘? testing’, sekali lagi cukup gunakan simbolnya saja untuk mengulangi pencarian.

Untuk mengganti, Anda memerlukan perintah yang lebih kompleks. Untuk mengganti satu ‘search’ dengan ‘replace’ pada baris yang sama, gunakan ‘:s/search/replace’. Untuk mengganti yang lain, gunakan ‘:s’ saja. Jika Anda ingin mengganti semua ‘search’ pada baris saat itu, tambahkan ‘/g’ pada akhir perintah. Perintah berikut: ‘:s/search/replace/g’ akan mengganti semua hasil pencarian ‘search’dengan ‘replace’ pada baris saat itu. Untuk mengganti semua ‘search’ pada seluruh file, gunakan ‘:s%’. Jadi mengetik ‘:%s/search/replace/g’, atau menambahkan ‘c’ setelah ‘/g’ akan membuat Vim meminta konfirmasi Anda pada waktu hendak mengganti item yang cocok.

Anda bisa menjalankan perintah shell apa pun dari Vim dengan menggunakan ‘:!’ diikuti oleh perintah Anda. Sebagai contoh, ‘:!ls’ akan menampilkan daftar direktori pada direktori saat itu (di mana Anda berada sebelum menjalankan Vim). Anda bahkan bisa menggunakan ‘:!vi’ untuk menjalankan Vim lain di dalam Vim Anda sekarang, tetapi itu bisa membingungkan. Cara lain, gunakan ‘:shell’ untuk menjalankan shell utuh.

Hal terakhir yang ingin kami perlihatkan adalah fitur unik pada KDE, yang memungkinkan Anda untuk menggunakan Vim sebagai editor teks default untuk semua aplikasi yang mendukungnya. Sebagai contoh, KWrite dan KMail memungkinkan Anda untuk memilih editor teks yang ingin digunakan untuk teks, dan melalui KDE Control Centre Anda bisa mengonfigurasi Vim.

Pastikan bahwa KVim atau GVim terinstalasi (beberapa distro, seperti Fedora, memnyebutnya XVim). Selanjutnya, buka KDE Control Centre, pilih daftar ‘KDE Component’, dan kemudian pilih ‘Vim Component Configuration. Anda mungkin perlu mengarahkannya ke biner Vim yang baru, yang biasanya /usr/X11R6/bin/gvim. Tekan Test untuk memastikan ia bekerja. Jika ya, sekarang Anda hanya perlu mengganti editor default ke Vim. Untuk melakukan itu, buka Component Chooser pada KDE Components, pilih ‘Embedded Text Editor’ dari daftar, kemudian ganti ke Vim. Selesai.

Meskipun Vim jauh lebih mudah dibanding rivalnya, Emacs, fokusnya pada editing teks berarti Anda tidak perlu menekan terlalu banyak tombol untuk menyelesaikan pekerjaan Anda. Sama juga, karena tidak ada menu atau ruang lain maka Anda bisa lebih banyak melihat teks pada layar.

menjadi tempat yang lebih baik untuk memulai karena di situ terdapat halaman info dengan pertanyaan mengenai penggunaan Emacs secara umum. Karena Emacs telah ada sejak lama, banyak pertanyaan yang telah ditanyakan. Jadi sudah hampir bisa dipastikan Anda akan menemukan jawaban di situ!

Ada beberapa perintah untuk menampilkan informasi mengenai perintah Emacs dan penggunaannya. Sebagai contoh, ‘C-h a’ memungkinkan Anda memasukkan perintah Emacs untuk mengetahui apa yang dilakukan. Jadi ‘C-h a’ kemudian ‘replace string’ dan [Enter] akan memberitahu Anda bahwa fungsi replace-string mencari dan mengganti teks. Anda bisa mendapatkan informasi suatu perintah dengan menggunakan ‘C-h c’, yang meminta Anda untuk memasukkan perintah lain. Sebagai contoh, ‘C-h c’ kemudian ‘C-h a’ menampilkan ‘C-h a runs the command apropos-command’.

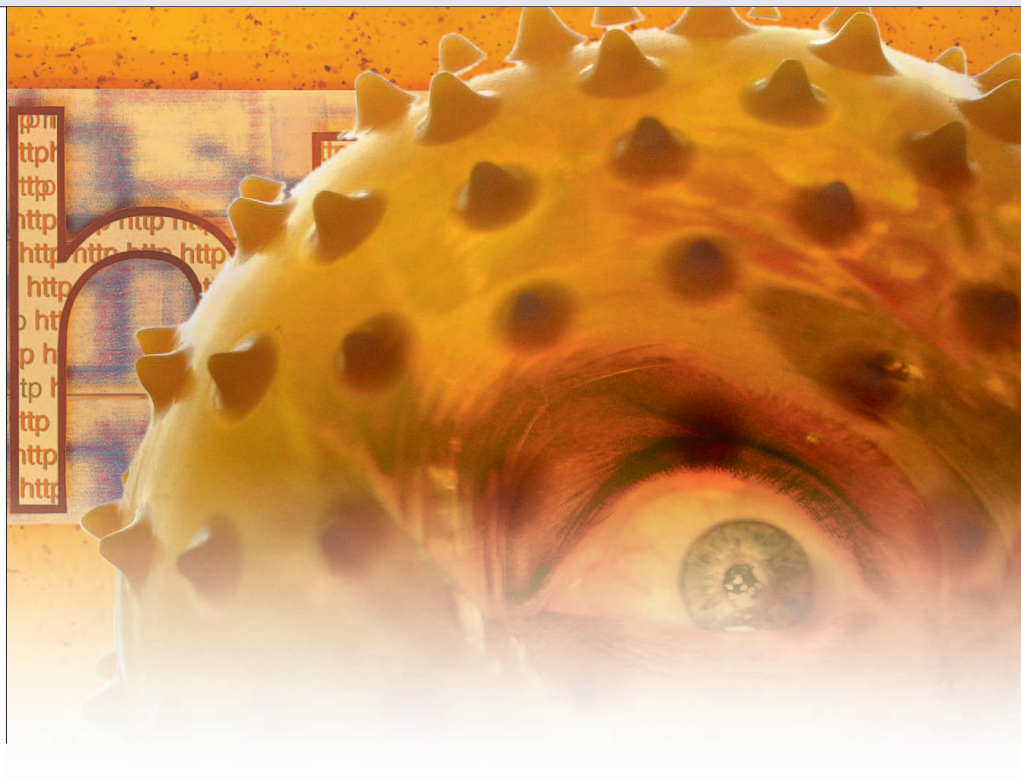
Satu perintah terakhir yang mungkin digunakan adalah ‘C-h b’ yang menampilkan semua penekanan tombol yang digunakan untuk suatu tindakan (*action*), dan juga yang mereka lakukan. Anda bisa mengetahui apa yang dilakukan masing-masing perintah dengan memindahkan kursor, dengan keyboard atau mouse, di atas nama perintah yang digaris bawah, dan menekan [Enter]. ■

LEBIH LANJUT

- **http://www.emacs.org/**
- **http://www.vim.org/**

Sistem Anda bertingkah sedikit aneh dan Anda pikir mungkin terinfeksi *spyware*. Kita lihat bagaimana tanda-tandanya!

Gunung Sarjono



Terinfeksi Spyware? Lihat Tanda-tandanya!

Anda mungkin pernah mendengar: "Komputer saya bertingkah aneh". Semua dari kurangnya *maintenance* reguler sampai program yang berbahaya bisa menjadi penyebab masalah, tetapi *spyware* juga bisa disalahkan. Dari sistem yang lambat sampai perubahan misterius terhadap *setting* Internet Anda, kali ini kita lihat tanda-tanda yang menunjukkan bahwa Anda terinfeksi spyware.

Visual

Tanda yang paling jelas dari sistem yang terinfeksi cenderung visual. Di antaranya, mungkin tidak ada yang lebih umum dibanding tanda *spyware* utama: jendela *pop-up*. Ini biasanya jendela *browser* dengan *style* Internet Explorer yang berisi iklan atau pesan peringatan. Ini biasanya muncul pada waktu Anda kali pertama *logon* ke komputer, atau pada waktu Anda menjalankan *web browser*.

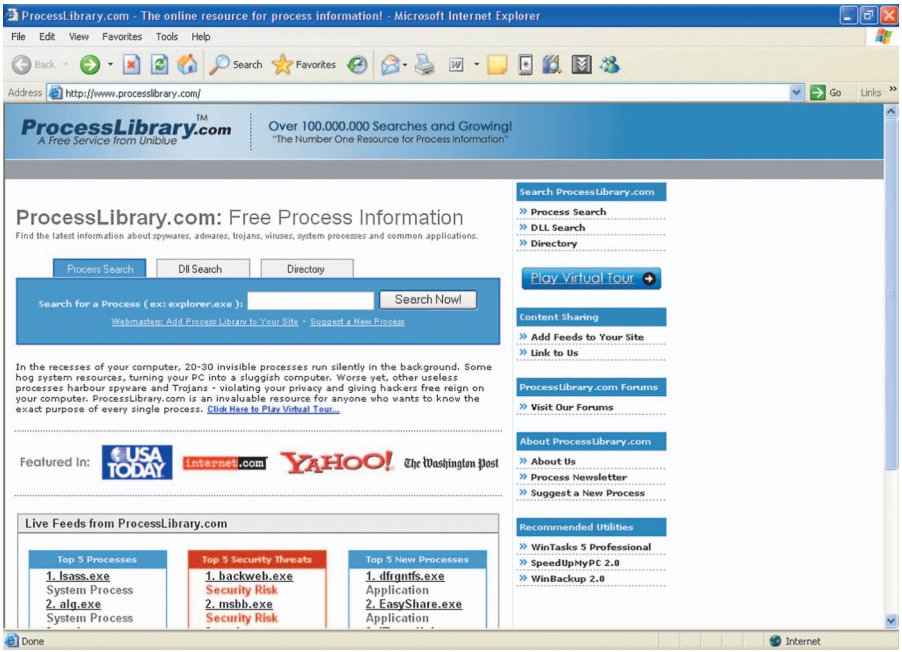
Perubahan terhadap *setting* browser tanda yang harus diperhatikan dalam mencari spyware. Sebagai contoh, jika Anda mengeset *home page* ke google (*http://www.google.com*), tetapi yang ditampilkan adalah halaman yang berbeda setiap kali Anda menjalankan browser, anggap saja sistem Anda terinfeksi. Ini terbukti benar terutama pada Internet Explorer, karena kontrol ActiveX yang di-*download* dari halaman web yang mencurigakan bisa melakukan perubahan tanpa sepengetahuan Anda.

Satu lagi tanda yang umum dari spyware adalah adanya *toolbar* pihak ketiga yang tidak dikenal pada Internet Explorer. Pada situasi tertentu mereka dimuat langsung di bawah bar alamat IE. Pada situasi lain, toolbar diinstalasi dan dimuat tetapi dicampur dekat toolbar *built-in*, supaya tidak menimbulkan kecurigaan. Untuk melihat apakah ada toolbar ekstra yang dimasukkan ke sistem Anda, buka Internet Explorer dan lihat *View, Toolbars*. Semua selain *Standard Buttons, Address Bar,* dan *Link* merupakan toolbar pihak ketiga, dan bisa saja spyware.

Satu visual terakhir yang perlu diwaspadai adalah icon *desktop* yang tidak dikenal atau tidak familiar. Sebagai contoh, misalnya *shortcut* ke situs porno, kasino Internet, atau program yang tidak familiar. Jika Anda menemukan ini, halus mereka dari desktop, lalu gunakan program anti-spyware untuk semua komponen yang perlu dihapus. Apapun yang Anda lakukan, jangan klik mereka—Anda bisa saja membuat sesuatunya lebih buruk.

Kinerja

Seiring dengan waktu, setiap komputer akan mengalami kelambatan dan *error*. Meskipun kedua "petunjuk" ini sering kali hanya indikasi perlunya melakukan *maintenance*—menghapus program yang tidak diperlukan, membatasi mana yang dijalankan secara otomatis, dan melakukan maintenance seperti defragmentasi—mereka juga sering kali menunjukkan adanya *spyware*.



***ProcessLibrary.com*—Sumber *online* untuk mengetahui informasi tentang proses.**

Sebagai contoh, Anda mungkin merasakan penurunan respon sistem keseluruhan secara dramatis, yang bisa saja akibat dari program spyware yang memakan memory pada waktu dijalankan secara *background*. Atau, mungkin Anda merasakan meningkatnya jumlah pesan error yang diterima. Pada kedua kasus, spyware bisa disalahkan, paling tidak pada tingkat tertentu. Ini benar terutama jika Anda tidak mempunyai kebiasaan sering menginstalasi software baru. Jadi, jika jauh lebih lambat dari biasanya (atau sesuatunya tidak bekerja seperti biasa), kini saatnya melakukan *scan* spyware pada komputer Anda untuk mengembalikan sesuatunya ke normal.

Di Belakang Layar

Petunjuk visual dan kinerja relatif mudah ditemukan, tetapi yang lain butuh sedikit usaha. Salah satu contoh adalah daftar situs yang di-*bookmark* pada Internet Explorer. Meskipun Anda sudah tidak lama menggunakannya (karena ganti ke Firefox misalnya), luangkan waktu untuk membuka IE dan melihat isi menu *Favorites*. Jika sistem Anda terinfeksi oleh *spyware*, Anda akan menemukan banyak *link* ke situs mencurigakan, mulai dari pornografi, judi, dan cara cepat untuk kaya. Kami sarankan untuk menghapus item secara manual, lalu melakukan scan. Biasanya, program anti-spyware tidak akan menghapus apapun dari daftar karena takutnya menghapus sesuatu yang mungkin Anda

FIREWALL: APAPUN CARA YANG DIGUNAKAN UNTUK TERHUBUNG KE INTERNET, ANDA MEMERLUKAN PERLINDUNGAN

■ Pernah ada anggapan bahwa *firewall* hanya digunakan dalam perusahaan besar—mereka digunakan supaya *user* Internet bisa terhubung ke sistem dalam jaringan privat. Namun, dengan semakin bertambahnya popularitas Internet, *hacker* dan pembuat *script* mulai menyadari bahwa ada target yang sangat mudah di luar sana, yaitu *end user* (yang menggunakan koneksi *dial-up* dan *broadband*), yang sering kali tidak mengamankan komputer mereka pada waktu *online*. Sama seperti Anda tidak mau meninggalkan pintu mobil tidak terkunci pada tempat parkir umum, maka sangat penting untuk mengunci user Internet dari komputer Anda dengan menggunakan firewall.

Yang Dilakukan Firewall

Pada tingkat paling dasar tugas *firewall* adalah untuk mengontrol *traffic* jaringan apa yang bisa memasuki atau meninggalkan PC Anda. Biasanya, firewall secara otomatis akan memblokir semua koneksi yang dilakukan user Internet ke komputer Anda, tetapi membolehkan *request* Internet yang berasal dari PC Anda. Dengan kata lain, firewall akan menghentikan user luar sehingga tidak dapat terhubung ke sistem Anda, sementara Anda bisa mengakses Internet tanpa larangan.

Konfigurasi *default* ini bekerja dengan baik bagi sebagian besar user, tetapi firewall pada dasarnya juga menyediakan kontrol yang lebih besar atas apa yang boleh memasuki atau meninggalkan sistem Anda. Sebagai contoh, misalnya Anda ingin memblokir semua *request outgoing* dari komputer Anda, kecuali untuk *service* biasa seperti *browsing* web, dan mengirim/menerima e-mail. Dengan konfigurasi ini, user yang mencoba menggunakan service MSN Messenger dari komputer Anda tidak akan bisa melakukannya.

Mempunyai firewall untuk melindungi sistem Anda adalah sangat penting. Alasan pertama adalah karena besarnya ancaman keamanan di mana sistem Windows rentan—sistem yang tidak terproteksi dan ter-*patch* sering kali bisa diserang oleh user Internet yang men-*scan range* alamat IP untuk mencari sistem yang lemah. Dengan adanya firewall, koneksi tersebut bisa ditolak—fitur ini dikenal sebagai *inbound protection*. Jika sistem Anda tidak diproteksi, user luar bisa mengambil alih komputer Anda, dari root sampai file pribadi, dan banyak lagi.

Kedua, firewall memungkinkan Anda mengontrol apa yang meninggalkan sistem Anda—fitur ini yang dikenal sebagai *outbound protection*. Ini penting karena sekarang spyware dan virus terus menyebabkan kekacauan pada sistem. Dengan firewall yang tepat, program spyware pada sistem Anda tidak akan bisa mengumpulkan dan meneruskan file peronal dan/atau data dari komputer Anda ke server di Internet, dan virus akan membutuhkan waktu lebih lama untuk meng-e-mail diri mereka sendiri ke kontak pada buku alamat Anda. Pada Internet sekarang ini, mempunyai kontrol atas

BERSAMBUNG...

FIREWALL: APAPUN CARA YANG DIGUNAKAN UNTUK TERHUBUNG KE INTERNET, ANDA MEMERLUKAN PERLINDUNGAN

apa yang keluar dari sistem Anda sama pentingnya dengan mempunyai kontrol atas apa yang masuk.

Windows Firewall

Jika Anda menggunakan Windows XP dan telah menginstalasi SP2, maka semua koneksi jaringan sistem Anda otomatis diproteksi oleh Windows Firewall (dengan asumsi Anda tidak menginstalasi program firewall lain). Meskipun Windows Firewall menawarkan *inbound protection* (dan memungkinkan Anda untuk memilih program atau service mana yang bisa menerima koneksi dari Internet user), ia tidak melakukan apa-apa untuk mengontrol apa yang keluar dari sistem Anda—ia kurang dalam hal kontrol *outbound traffic*.

Jadi, jika PC Anda terinfeksi oleh spyware, ia bisa berkomunikasi melalui Internet tanpa larangan. Informasi yang dikirimkan dari komputer Anda bisa saja tidak "berbahaya" seperti detail situs web yang telah Anda browsing, tetapi bisa juga meliputi informasi pribadi seperti nomor kartu kredit, atau kumpulan penekanan keyboard yang Anda lakukan.

Apakah itu berarti Windows Firewall tidak menawarkan proteksi yang cukup? Bukan begitu. Windows Firewall bisa jadi semua proteksi firewall yang Anda butuhkan, tetapi hanya jika Anda betul-betul yakin bahwa sistem Anda tidak terinfeksi oleh virus, spyware, atau ancaman lainnya. Pada suatu sistem yang bersih, Anda tidak perlu memikirkan traffic yang ditujukan ke Internet, karena itu semua di-*request* oleh Anda. Namun, ancaman seperti spyware dan virus sangat nyata dan terus menginfeksi sebagian besar deskop PC user. Dengan demikian, sebagian besar user memerlukan *inbound* dan *outbound protection*.

Firewall Alternatif

Jika Anda khawatir bahwa sistem tidak cukup diproteksi dengan Windows Firewall (atau jika Anda tidak menjalankan Windows XP), maka sekarang waktunya untuk menginstalasi *software firewall* pada PC Anda. Banyak pilihan yang tersedia, seperti ZoneAlarm, Kerio Personal Firewall, dan lainnya. Produk ini menawarkan *inbound* dan *outbound protection* secara lengkap, dan memberi Anda kontrol atas elemen seperti program mana yang diberi akses ke Internet.

Versi bayar dari produk ini datang dengan fitur tingkat lanjut yang luas (seperti kemampuan untuk memproteksi informasi kartu kredit Anda dan men-scan email), kebanyakan tersedia dalam versi *free* yang juga menawarkan inbund dan outbound protection secara komprehensif, belum lagi notifikasi pada layar memperingati Anda atas *event* yang penting, seperti koneksi dari user luar, program yang mencoba terhubung ke Internet sendiri, dan banyak lagi.

butuhkan pada masa yang akan datang.

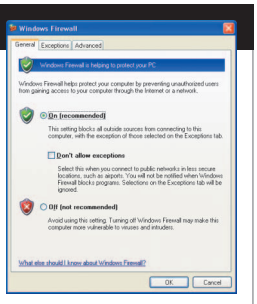
Indikator infeksi yang lain adalah program sekuriti seperti *firewall*, antispyware atau antivirus di-*disable* atau *shutdown*. Spyware (dan virus) tertentu mempunyai komponen untuk men-*disable* proteksi Anda sebagai cara untuk memastikan kelanjutan hidup mereka. Icon pada *System tray* bisa menjadi petunjuk yang baik untuk mengetahui apakah program tersebut aktif, demikian juga dengan *Security Center* pada Control Panel XP.

Sebagian alasan mengapa spyware sering kali tidak diketahui adalah karena Windows memungkinkan program untuk dijalankan secara *background*. Jika Anda benar-benar ingin tahu apa yang berjalan pada sistem, lihat tab *Process* pada *Task Manager*. Di situ Anda akan menemukan nama setiap proses yang berjalan pada PC, termasuk program spyware yang aktif. Anda akan memerlukan sedikit bantuan untuk mengetahui proses mana yang benar (sah) dan mana yang tidak, tetapi *ProcessLibrary.com* akan membantu Anda menemukan jawabannya.

Tagihan Telepon Membengkak

Petunjuk terakhir bahwa sistem Anda terinfeksi oleh spyware adalah yang paling mengejutkan, dan datang melalui pos. Kita berbicara tentang tagihan telepon dan jika sistem Anda terinfeksi oleh yang dikenal dengan program dialer, maka Anda tidak akan senang pada waktu menerimanya. Program ini biasanya diinstalasi melalui Web plug-in atau bersama dengan program yang kelihatannya tidak bermasalah (sering kali dihubungkan dengan kasino online atau situ pornografi). Begitu mendapatkan jalan untuk masuk ke sistem, mereka menggunakan modem Anda untuk melakukan panggilan jarak jauh ke tempat di seluruh dunia, membuat tagihan internasional yang sangat besar. ■

DI DALAM WINDOWS FIREWALL



- Untuk mengecek apakah Windows Firewall melindungi sistem Anda, buka *Control Panel* dan cari applet Windows Firewall pada *Classic View*. Jika ada, buka untuk melihat tab *General*, yang seharusnya diset ke *On* (*recommended*). Jika tidak ada, instalasi SP2.
- Anda bisa mengontrol program dan *service* mana yang diberi *inbound protection* dari tab *Exceptions*. Beri tanda centang (✓) item—pada waktu item tidak dicentang (✓), koneksi diblokir. Anda juga bisa membuat daftar pengecualian sendiri.
- Gunakan tab *Advanced* untuk meng-*enable* atau *disable* service, mengonfigurasi *setting* file log, dan banyak lagi. Pastikan *logging* dilakukan jika Anda ingin melacak koneksi inbound yang dilakukan ke PC Anda, misalnya.

LEBIH LANJUT

- **http://www.kerio.com/**
- **http://www.processlibrary.com/**
- **http://www.zonelabs.com/**

Menyadap pembicaraan orang adalah tindakan ilegal. Sampai saat ini pun, kegiatan penyadapan untuk proses penyidikan tidak dapat dilakukan sembarangan. Perlu dilengkapi dengan bukti yang cukup sampai sebuah lembaga boleh melakukan tindakan penyadapan.

Fadilla Mutiawarati

Teknologi Sederhana Dapat Menyadap Telepon Anda

Menyadap telepon merupakan pelanggaran hak asasi manusia yang diakui secara internasional. Artinya, aktivitas penyadapan telepon di manapun tidak dibenarkan. Aktivitas ini sudah pasti mengganggu privasi seseorang sehingga sangat ditentang. Namun di lain sisi, menyadap telepon dapat menjadi cara yang sangat efektif untuk mengetahui sebuah informasi yang sangat rahasia. Sehingga terkadang proses penyadapan dibenarkan. Khususnya untuk membantu proses penyelidikan pada kasus yang sangat berbahaya/besar. Aktivitas menyadap juga dapat menjadi cara yang efektif mengontrol penggunaan telepon. Bahkan sebagian orang ada juga yang menggunakan kegiatan menyadap ini sebagai salah satu sarana pencuran pulsa.

Yang paling besar memiliki kesempatan untuk melakukan aktivitas ini adalah perusahaan telekomunikasi. Karena di sanalah semua bentuk komunikasi bermuara. Namun, bukan berarti orang awam tidak dapat melakukannya. Proses penyadapan dapat dilakukan dengan sangat cepat dan mudah. Meskipun semakin sederhana, semakin mudah diketahui.

Kemudahan aktivitas sadap menyadap ini membuat seorang informan (penjahat maupun pemerintah) atau mata-mata melakukan komunikasi dengan menggunakan bahasa-bahasa sandi.

Pada Jaringan Analog

Seperti yang tadi telah diungkapkan bahwa menyadap adalah aktivitas yang sangat mudah dilakukan. Anda tidak perlu menjadi seorang detektif atau teknisi untuk dapat menyadap telepon. Bahkan anak-anak pun dapat dengan mudah melakukannya. Hanya saja tidak semua aktivitas penyadapan bisa dikatakan aman.

Aman atau tidaknya kegiatan penyadapan sangat bergantung kepada teknik dan perangkat yang digunakan. Semakin sederhana, maka semakin mudah diketahui. Sedangkan, tingkat kesulitan aktivitas ini sangat bergantung juga kepada sistem telekomunikasi yang digunakan oleh target atau korban.

Jaringan analog adalah yang paling rentan. Artinya, lebih mudah disadap dibandingkan jaringan telekomunikasi digital. Hal ini disebabkan dengan teknologi digital sinyal yang ditransmisikan kana terlebih dahulu melalui proses pengodean. Sehingga siapapun yang mencurinya tidak akan mudah mendengarkan suara yang sebenarnya. Karena harus terlebih dahulu mengubah kode-kode yang ada. Berbeda dengan sinyal analog yang bersifat langsung. Hal inilah yang memudahkan telekomunikasi dengan sinyal analog mudah dicuri. Karena seorang pencurinya tidak perlu repot mengubah atau membaca kode seperti pada transmisi digital.

Coba Anda bongkar pesawat telepon yang ada di ada di rumah. Dari boks

Dengan peralatan sederhana, sebuah pesawat telepon sudah dapat disadap.

saluran telepon sampai pesawat telepon hanya akan ada sebuah kabel dengan dua kawat tembaga di dalamnya yang dapat Anda temui. Biasanya kedua kawat tembaga ini dilapisi plastik yang berbeda warna satu sama lain. Satu kawat tembaga tempat mengalirnya sinyal ke dalam dan satu lagi untuk membawa sinyal keluar. Jika kedua kabel ini dikaitkan ke sebuah pesawat telepon lain, maka Anda dapat langsung mendengarkan percakapan pada telepon tersebut.

Konsep ini biasanya digunakan untuk rumah-rumah yang memasang teleponnya secara paralel hanya dengan bantuan *spliter* sederhana. Satu spliter dapat digunakan untuk memaralelkan sampai tiga telepon sekaligus, tergantung dari lubang keluarnya. Sedangkan lubang masuk hanya akan ada satu saja di belakangnya.

Adalah jumlah kabel yang sama yang akan Anda temui bila Anda membongkar sebuah gagang telepon biasa. Dan seperti layaknya pada sebuah spliter, Anda pun dapat menarik kabel dari dalam gagang tersebut untuk dapat mendengarkan pembicaraan. Masing-masing kabel mengalirkan sinyal ke speaker dan dari mikrofon.

Cara dan Alat

Dari keterangan tadi, tentu Anda sudah dapat membuat kesimpulan bahwa siapapun yang akan menyadap telepon Anda dapat melakukannya dengan dua cara. Melalui kabel di luar atau langsung dari gagang telepon.

Namun, perlu Anda ketahui bahwa kegiatan penyadapan tidak akan dikatakan kejahatan bila dilakukan sepengetahuan si pengguna telepon. Kegiatan ini hanya dapat digolongkan sebagai kegiatan kejahatan bila dilakukan tanpa sepengetahuan si pengguna telepon.

Penyadapan dapat saja sah bila dilaksanakan untuk kepentingan keamanan atau membatasi pembicaraan. Misalnya saja pada telepon umum. Jika penyadapan dilakukan pada telepon umum dengan meletakkan pemberitahuan yang jelas, maka si pengguna telepon umum tersebut pasti akan merasa canggung untuk melakukan pembicaraan berbau seks dan sara apalagi rencana kejahatan.

Untuk merekam atau menyadap pembicaraan yang seperti ini, Anda hanya perlu menyediakan alat-alat yang sederhana. Yaitu sebuah tape recorder, sebuah spliter, dan kabel telepon. Caranya cukup sambungkan sebuah spliter yang membelah antara peswat telepon yang akan disadap dengan satu kabel menuju tape recorder. Lalu jalankan selalu tape recorder setiap kali ada orang yang menggunakan telepon.

Jika ingin memudahkan pengoperasian, Anda dapat menambahkan sebuah sensor yang dapat membantu tape decoder untuk bekerja secara otomatis. Atau menggunakan tape decoder yang memiliki sensor suara. Sehingga tape hanya akan merekam bila ada pembicaraan saja.

Dengan cara ini, seseorang harus selalu rajin mengontrol isi tape. Jangan sampai kehabisan. Dan harus rajin untuk membolak-balik tape. Lain halnya jika menggunakan teknologi digital dan langsung menyimpan file pembicaraan ke komputer. Dengan cara ini, data dapat lebih banyak ditampung ketimbang dengan tape biasa. Sekarang ini sudah banyak komputer atau modem yang melengkapi paketnya dengan aplikasi telepon serta phone recorder.

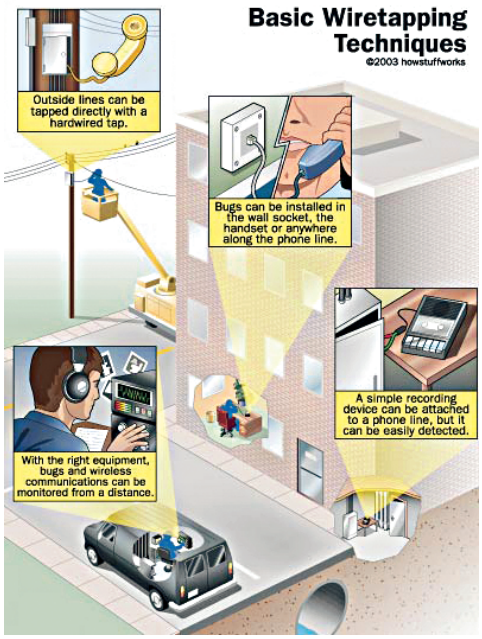
Kriminal

Untuk kegiatan kriminal sendiri, cara seperti ini tidak pernah dilakukan, karena seorang pengguna telepon dapat mudah mengetahuinya. Apalagi jika telepon-telepon tersebut digunakan oleh orang-orang penting dengan staf keamanan yang terlatih.

Untuk kegiatan kriminal, kegiatan penyadapan dilakukan dengan lebih lihai. Misalnya saja dengan meletakkan sebuah alat pada boks saluran telepon agar tidak mudah terlihat. Atau jika ternyata telepon yang digunakan adalah telepon digital, maka bisa saja pengintai melakukan penyadapan dengan menggunakan alat kecil yang di sebut *bug*. Bug diletakkan pada gagang telepon.

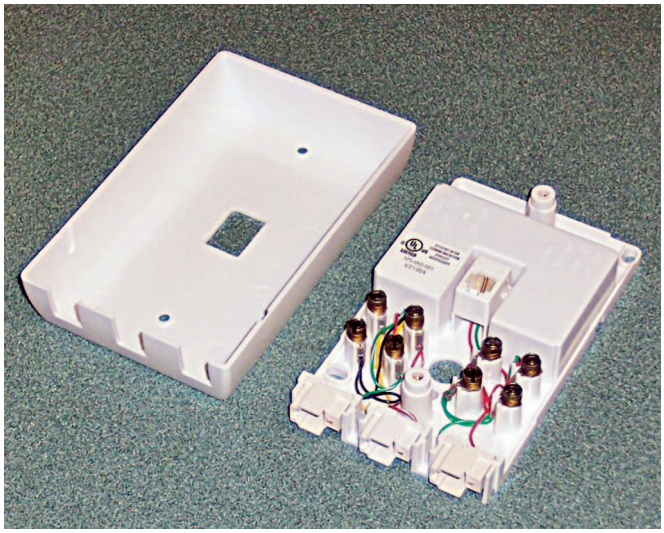
Bug sifatnya tanpa kabel. Sehingga korban tidak akan mengetahui apakah teleponnya sedang disadap atau tidak. Bug berbentuk sangat kecil dan memiliki dua kaki kabel yang masing-masing melekat pada masing-masing kabel dalam gagang telepon. Bug mengirimkan datanya dengan bantuan frekuensi radio kepada *receiver*-nya. Data yang dikirimkan oleh bug dapat direkam atau dapat langsung didengarkan oleh penerima sinyal.

Keberadaan bug sangat popular saat ini dalam penyadapan telepon. Namun, bukan berarti bug tidak dapat dideteksi. Dengan alat sinyal detektor, keberadaan bug juga dapat diketahui. Dan sebagian yang memiliki staf keamanan yang tinggi dapat mengetahuinya. Sedangkan untuk orang yang terlalu lihai, biasanya tidak menyadari bahwa dirinya sedang disadap.



Penyadapan dapat dilakukandnegan berbagai cara. Sumber gambar: *Howstuffworks.com*.

Label yang diberikan pada telepon yang disadap.



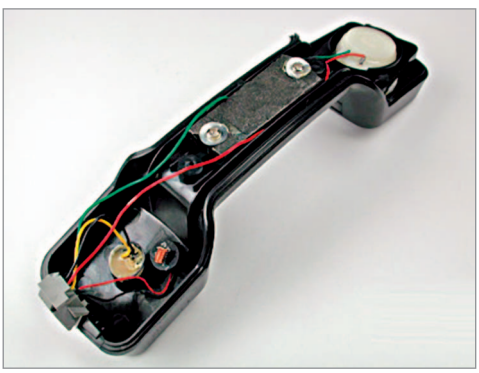
Phone spliter, cara lama memaralelkan telepon.

Sejak Perang Dunia Pertama

Kegiatan sadap menyadap sudah ada sejak masa perang dunia pertama. Pada awalnya memang untuk kebutuhan mata-mata pemerintahan sebuah negara. Namun, kemudian berkembang. Tidak hanya dunia peperangan dan politik saja yang melakukan kegiatan penyadapan. Dunia bisnis pun banyak dipenuhi dengan kegiatan penyadapan ini.

Oleh sebab itu, umumnya para mata-mata atau orang-orang tertentu yang merasa dirinya rawan dengan penyadapan sangat hati-hati dalam berbicara, umumnya mereka menggunakan kode-kode tertentu dalam percakapan. Baik melalui telepon maupun tatap muka.

Hal ini disebabkan penyadapan tidak hanya dapat dilakuan secara fisik berdekatan dengan korban, tetapi juga dapat dilakuan tanpa jejak dengan menggunakan alat detektor khusus yang dapat ditembakkan dari jarak jauh.



Bagian dalam gagang telepon yang sudah disadap dengan *bug*.

Dan tidak hanya pembicaraan melalui telepon PSTN saja yang dapat disadap. Pembicaraan dengan menggunakan telepon genggam pun sangat rawan dengan penyadapan. Bahkan cenderung lebih mudah. Cukup dengan penyurian sinyal, maka penyadapan dapat dilakukan. Coba saja Anda gunakan sebuah pesawat radio xxx yang biasa digunakan oleh polisi dan penggemar radio amatir. Kadang mereka dapat secara tidak sengaja pembicaraan telepon yang dilakukan dengan ponsel.

Namun, lain halnya jika pembicaraan dilakukan dengan menggunakan telepon CDMA. Karena ada proses pengodean yang tidak terjadi pada pesawat GSM. Sehingga pembicaraan dengan telepon CDMA lebih aman. Tingkat keamanan pada CDMA sudah lebih dulu dikenal oleh dunia militer ketimbang masyarakat awam.

Apakah Telepon Anda juga Disadap?

Tagihan telepon melonjak atau Anda merasakan kualitas suara pembicaraan terasa aneh. Bisa saja telepon Anda tersadap. Namun, jangan terburu buruk sangka. Siapa tahu ternyata Anda sendirilah sebagai pelakukanya. Cobalah untuk memeriksa jaringan telepon di rumah. Bila Anda memaralelkan telepon hanya dengan menggunakan pembagi jaringan biasa hal tentu saja sangat rentan, karena siapa saja di ujung pesawat sana dapat mendengarkan percakapan Anda kapan saja.

Oleh sebab itu, bila Anda akan membagi jaringan di rumah atau ingin menggunakan lebih dari satu pesawat untuk satu nomor, Anda dapat menggunakan Mini PABX. Dengan alat ini, setiap saluran hanya akan digunakan oleh satu pesawat saja. Pesawat lain tidak dapat mendengarkan bila pesawat yang lain sudah menerimanya.

Dan bila ternyata setelah menggunakan Mini PABX kualitas suara tetap saja kurang baik atau kurang kuat, hubungi pusat pelayanan telepon untuk memintanya memeriksa jaringan telepon Anda di boks saluran telepon. Siapa tahu ada yang melakukan kecurangan di sana, atau ada saluran yang saling berinterferensi.

Tidak jarang persinggungan antar-kabel pada perangkat penghubung juga dapat menyebabkan kebocoran yang artinya, Anda dapat mendengarkan pembicaraan orang lain atau sebaliknya orang lain dapat mendengarkan pembicaraan Anda.

Proses penyadapan yang sederhana selalu meninggalkan jejak. Oleh sebab itu, Anda tidak perlu khawatir. Lain halnya bila proses penyadapan dilakukan dengan alat yang lebih rumit. Misalnya dengan memasukkan *bug* ke dalam pesawat telepon. Hal ini tentu akan sulit dirasakan. Kecuali Anda membongkar pesawat Anda. ■

LEBIH LANJUT

- **www.spybusters.com**