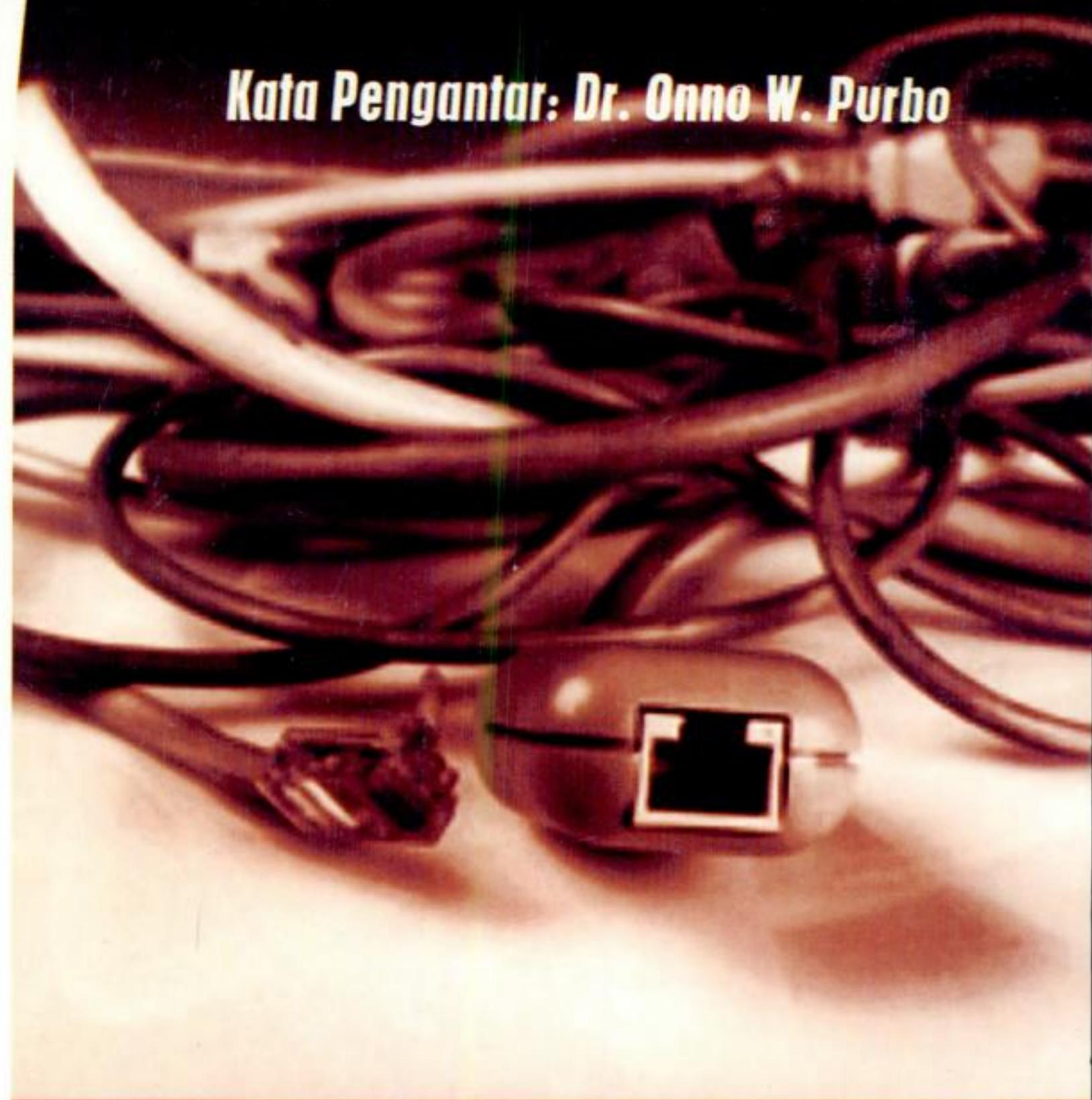


Kata Pengantar: Dr. Onno W. Purbo



PENERBIT ANDI



PENGENALAN PROTOKOL
JARINGAN
Wireless
KOMPUTER

EDI S. MULYANTA, S.Si.

Pengenalan Protokol Jaringan Wireless Komputer

Oleh: Edi S. Mulyanta, S.Si

Hak Cipta © 2005 pada Penulis.

Editor : Th. Arie Prabawati

Setting : Sri Mulanto

Desain Cover : Yossy S.P. Hutaurok

Korektor : Wiwin Dwi Lestari/Aktor Tunas Agung

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.

Penerbit:

C.V. ANDI OFFSET (Penerbit ANDI)

Jl. Beo 38-40,

Telp. (0274) 561881 (Hunting), Fax. (0274) 588282 Yogyakarta 55281

Percetakan:

ANDI OFFSET

Jl. Beo 38-40,

Telp. (0274) 561881 (Hunting), Fax. (0274) 588282 Yogyakarta 55281

Perpustakaan Nasional: Katalog dalam Terbitan

Mulyanta, Edi S

*Pengenalan Protokol Jaringan Wireless Komputer/
Edi S. Mulyanta; – Ed. I. – Yogyakarta: ANDI;*

09 - 08 - 07 - 06

xii + 260 hlm .; 16 x 23 Cm.

10 9 8 7 6 5 4 3 2

ISBN: 979 - 731 - 836 - 2

I. Judul

I. Computer Networks

DDC'21: 004. 65

Daftar Isi

KATA PENGANTAR	v
DAFTAR ISI	VII
BAB 1 PENDAHULUAN	1
1.1 JARINGAN	3
1.2 PROTOKOL	5
1.3 ARSITEKTUR JARINGAN	14
1.3.1 TCP/IP	15
1.3.2 Model Referensi Open Systems Interconnection (OSI)	16
1.3.3 Layer Protokol	18
1.4 PERTANYAAN	20
BAB 2 KONSEP DASAR PERTUKARAN DATA DI JARINGAN KOMPUTER	21
2.1 PROTOKOL KOMUNIKASI	23
2.2 KOMUNIKASI PEER TO PEER	25
2.3 KOMUNIKASI ANTARSISTEM MODEL OSI	27
2.3.1 Interaksi Antarlayer	27
2.3.2 Pertukaran Informasi	28
2.4 ARSITEKTUR JARINGAN WIRELESS	31
2.4.1 Sinyal Digital Informasi	33
2.4.2 Udara Sebagai Media Pertukaran Data	34
2.5 PERTANYAAN	35
BAB 3 LAYER PHYSICAL (PHY)	37
3.1 KONSEP LAYER FISIK	37
3.1.1 Internetwork	38
3.1.2 Protokol LAN	39
3.1.3 Peralatan pada Layer Fisik	40
3.1.4 Backbone dan Segmen	41
3.2 LAYER FISIK DI JARINGAN WIRELESS	42
3.2.1 Proyek 802	43
3.2.2 IEEE 802.11	46
3.2.3 Channel	51
3.2.4 Range dan Performa	52
3.2.5 Wi-Fi (Wireless Fidelity)	52

<u>3.2.6 Ad Hoc</u>	53
3.2.7 Client/Server dan Access Point	54
<u>3.2.8 Pengembangan Konfigurasi Wireless</u>	55
3.3 INFRASTRUKTUR JARINGAN FISIK WIRELESS	56
3.3.1 Memahami Card Internal 802.11	59
<u>3.3.2 Keamanan Jaringan Wireless</u>	62
<u>3.3.3 Pencegahan Keamanan Jaringan yang Lain</u>	63
<u>3.4 ANTENA</u>	64
<u>3.4.1 Dasar Antena</u>	64
3.4.2 Sinyal dan Pengukuran Noise	67
3.4.3 Antena pada Wireless LAN	68
<u>3.4.4 Metode Penyebaran Spektrum</u>	71
<u>3.5 PENGATURAN AKSES DENGAN ACCESS POINT</u>	75
3.5.1 Konfigurasi Akses	77
3.5.2 Beberapa Option di Access Point	78
3.6 TOPOLOGI JARINGAN WIRELESS	81
3.6.1 Independent Basic Service Set (IBSS)	81
<u>3.6.2 Basic Service Set (BSS)</u>	82
<u>3.6.3 Extended Service Set (ESS)</u>	82
3.7 PERTANYAAN	83
BAB 4 DATA LINK	85
4.1 FORMAT INFORMASI DATA LINK	85
4.1.1 Frame	86
4.1.2 Manajemen Frame	87
<u>4.1.3 Struktur Paket</u>	89
4.1.4 Manajemen dan Kontrol Paket	90
4.2 MEMAHAMI LAYER DATA LINK	90
4.2.1 MAC Sublayer	92
4.2.2 Layer MAC pada 802.11	93
<u>4.2.3 Proses Komunikasi</u>	94
4.2.4 Fungsi Layer MAC 802.11	96
4.2.5 Pengalamatan pada MAC	99
4.3 PERALATAN PADA DATA LINK	101
4.3.1 Bridge	101
4.3.2 Switch	103
4.4 MEDIUM ACCESS	103
4.4.1 Carrier Sense/Multiple Access With Collision Detection (CSMA/CD)	103
<u>4.4.2 Token Passing</u>	104

4.4.3 Carrier Sense/Multiple Access With Collision Avoidance (CSMA/CA)	105
4.5 KEAMANAN LAYER DATA LINK.....	107
4.6 PERTANYAAN	108
BAB 5 LAYER NETWORK.....	109
5.1 KONSEP LAYER NETWORK	109
<u>5.1.1 Pengalamatan pada Layer Network.....</u>	<u>110</u>
<u>5.1.2 Alamat Hierarki dan Alamat Flat.....</u>	<u>110</u>
5.1.3 Pemberian Alamat	111
5.1.4 Alamat dan Nama	112
5.2 ROUTING.....	112
5.2.1 Algoritma Routing	114
5.2.2 Pengukuran Routing.....	118
5.3 PERALATAN PADA LAYER NETWORK.....	119
5.3.1 Router.....	120
5.3.2 Brouter.....	120
5.3.3 Layer 3 Switch	120
5.4 PROTOCOL NETWORK.....	120
5.4.1 Interior Gateway Routing Protocol (IGRP)	121
5.4.2 Enhanced IGRP	122
5.4.3 Open Shortest Path First (OSPF).....	122
5.4.4 Border Gateway Protocol (BGP).....	123
5.4.5 Routing Information Protocol (RIP).....	123
5.5 TEKNIK ROUTING PADA JARIGAN WIRELESS.....	124
5.5.1 Routing pada Wireless Ad Hoc.....	124
5.5.2 Dynamic Source Routing.....	129
5.6 KEAMANAN LAYER NETWORK	130
<u>5.7 PERTANYAAN</u>	<u>131</u>
BAB 6 PAN, LAN, MAN DAN WAN WIRELESS	133
<u>6.1 PERSONAL AREA NETWORK.....</u>	<u>134</u>
6.1.1 Teknologi Wireless PAN	135
6.1.2 IrDA	136
<u>6.1.3 Bluetooth</u>	<u>141</u>
6.2 LOCAL AREA NETWORK	147
6.2.1 Wireless LAN	147
6.2.2 Hotspot.....	148
6.2.3 Fungsi dan Fitur Komponen Hotspot.....	150
<u>6.3 METROPOLITAN AREA NETWORK</u>	<u>154</u>
<u>6.3.1 Wireless MAN</u>	<u>154</u>

6.3.2 Pengembangan MAN dengan Wi-Fi Mesh Networking	158
6.3.3 WIMAX Sebagai Pilihan Pengembangan MAN.....	159
6.4 WIDE AREA NETWORK.....	160
6.4.1 Wireless WAN.....	160
6.4.2 Bentuk Komunikasi WAN.....	161
6.4.3 Cellular-Based Wireless WAN	162
6.4.4 Teknologi Wireless WAN	169
6.5 PERTANYAAN.....	172
BAB 7 KEAMANAN JARINGAN WIRELESS.....	173
7.1 MEMAHAMI RISIKO	175
7.1.1 Serangan Penyusupan.....	176
7.1.2 Bypass Monitoring Jaringan	179
7.1.3 Jamming atau Denial of Service (DoS).....	182
7.1.4 Serangan Client to Client.....	184
7.1.5 Brute Force Attack pada Access Point.....	184
7.1.6 Enkripsi.....	184
7.1.7 Kesalahan Konfigurasi	186
7.1.8 Man in the Middle Attacks	189
7.2 WEP (WIRED EQUIVALENT PRIVACY)	191
7.2.1 Initialization Vector (IV)	192
7.2.2 CRC 32.....	193
7.2.3 Operasi WEP	193
7.2.4 Kelemahan WEP	194
7.2.5 Penggunaan WEP	196
7.2.6 Pengembangan WEP.....	197
7.2.7 Crack pada WEP	199
7.2.8 Wi-Fi Protected Access (WPA).....	201
7.2.9 Virtual Private Networks (VPN)	202
7.2.10 PKI (Public Key Infrastructure)	207
7.3 AUTENTIKASI PADA WLAN.....	207
7.3.1 Autentikasi Mutual.....	208
7.3.2 Remote Authentication Dial-In User Service (RADIUS).....	208
7.3.3 Autentikasi 802.11	209
7.3.4 Autentikasi 802.1X.....	210
7.4 MANAJEMEN WLAN.....	212
7.4.1 Keamanan Menggunakan Sensor RF Terdistribusi.....	213
7.4.2 Remote Analysis pada WLAN	214
7.5 MITIGASI ACCESS POINT	215
7.5.1 Mencegah Access Point Liar.....	216
7.5.2 Deteksi Access Point Liar	217

7.5.3 Deteksi secara Wireless	218
7.5.4 Deteksi dari Jaringan Wired.....	218
7.6 PERTANYAAN	221
BAB 8 MEMBANGUN JARINGAN WIRELESS (HOTSPOT)	223
8.1 MEMBANGUN JARINGAN 802.11	223
8.1.1 Standar WLAN.....	224
8.1.2 Hotspot dan Pola Dasar Topologinya	225
8.1.3 Populasi Pemakai dan Model Pemakai.....	227
8.1.4 Faktor Bangunan dan Gedung.....	230
8.1.5 Keamanan dan Kenyamanan Wireless LAN	233
8.1.6 Langkah Terakhir.....	236
8.2 STUDI KASUS HOTSPOT SEDERHANA.....	237
8.2.1 Setup Awal	238
8.2.2 Konfigurasi IP Access Point.....	239
8.2.3 Basic Setup.....	239
8.2.4 Keamanan	240
8.2.5 Setup Client.....	242
8.3 PERTANYAAN	245
GLOSSARY.....	247
DAFTAR PUSTAKA.....	257

Bab 1

Pendahuluan

Wireless Connects You Anywhere

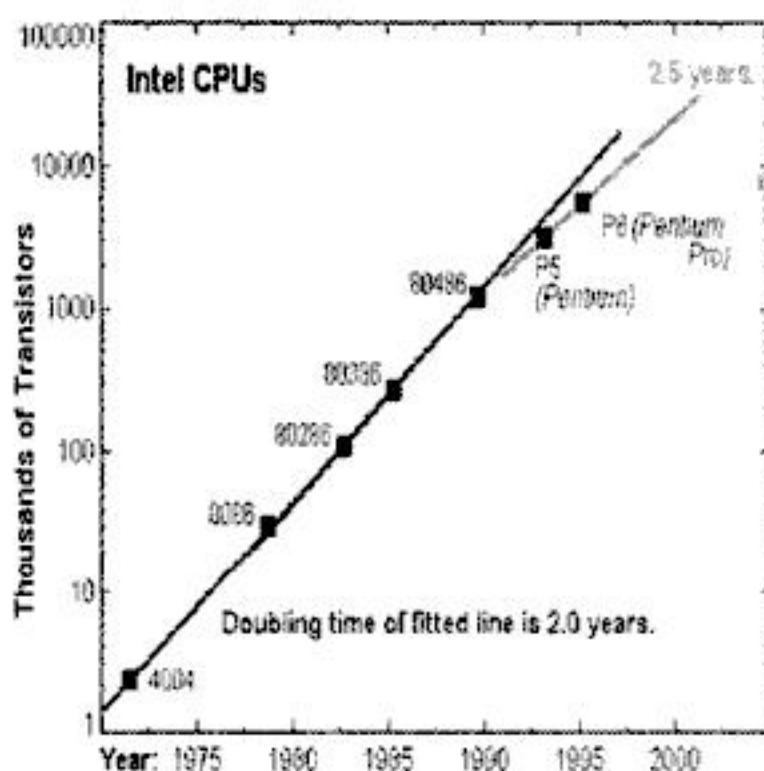
Tanpa disadari sebenarnya kehidupan manusia tidak dapat terlepas dari kebutuhan untuk saling berbagi dalam segala hal. Kemampuan teknologi telah menjawab berbagai tantangan manusia untuk saling berinteraksi secara *real time*, di mana batas antara jarak, waktu, dan ruang bukanlah penghalang bagi keinginan manusia untuk saling berkomunikasi.

Era digital telah merambah ke segala bidang, sehingga hampir tidak ada celah dalam kehidupan manusia yang tidak berhubungan dengan teknologi digital. Keinginan manusia untuk menyadari keberadaannya secara relatif dengan manusia yang lain menjadi obsesi yang tidak berlebihan, di mana sinergi dari kesadaran untuk saling berbagi pakai tersebut akan dapat memberikan kemudahan dalam menjalani kehidupan.

Komputer telah mendorong terjadinya revolusi di bidang teknologi informasi, di mana semua manusia menyadari pentingnya informasi sebagai suatu kebutuhan aktualisasi manusia dalam hal berbagi satu dengan yang lain. Perkembangan teknologi komputer telah memberikan kemudahan dalam semua hal karena secara fisik komputer telah semakin menyatu dalam kehidupan sehari-hari manusia. Semakin berkembangnya industrialisasi perangkat keras komputer membuat harga komputer semakin terjangkau oleh semua lapisan strata ekonomi manusia dengan kecepatan pengolahan data yang semakin meningkat secara signifikan.

Gordon Moore dari Intel telah melakukan observasi yang sangat penting di tahun 1965, enam tahun sejak ditemukannya transistor planar. Observasinya menghasilkan pernyataan tentang “akan berlipatnya kepadatan transistor yang dapat dibuat setiap tahunnya”. Pernyataan

tersebut selama hampir lebih dari 30 tahun disebut 'Moore's Law' atau Hukum Moore, dan masih tetap relevan hingga saat ini. Menurut Intel "tidak ada hal teoritis maupun praktis yang dapat menghindari Hukum Moore tersebut". Dengan menggunakan Hukum Moore, dapat diperkirakan hingga tahun 2012 Intel akan mampu mengintegrasikan satu miliar transistor yang akan beroperasi hingga 10 GHz dengan performa hingga 100.000 MIPS. Peningkatan ini relevan dengan pertumbuhan jumlah transistor dari prosesor 386 hingga Pentium II.



<http://www.physics.udel.edu/~watson/scen103/intel.html>

Gambar 1-1 Hukum Moore pada CPU Intel

Relevansi dari Hukum Moore tentunya telah diimbangi dengan berbagai kerja keras manusia dalam menghasilkan media yang dibutuhkan manusia pada masa yang akan datang, yaitu media pertukaran informasi. Hukum Moore selalu terbukti, karena tanpa sadari hukum ini telah menjadi target produksi dan *deadline* yang harus dipenuhi oleh Intel sendiri dalam menjajakan sejumlah transistor ke dalam IC produksi mereka.

Kesadaran akan berbagi pakai manusia beriringan dengan ambisi untuk dapat saling terkoneksi bermacam-macam jenis komputer dalam sebuah sistem jaringan dan sebuah sistem yang terdistribusi. Pada abad ini, kunci perkembangan teknologi komputer ada pada kemampuannya dalam mempersatukan informasi, melakukan proses informasi, dan mendistribusikan informasi.

Industri komputer dalam perkembangannya merupakan industri yang paling muda jika dibandingkan dengan teknologi industri lain, seperti industri mekanik, automobile, dan transportasi, akan tetapi kemajuan perkembangannya dapat dikatakan spektakuler dalam memengaruhi kehidupan manusia. Apabila kita melakukan *flash back* ke era awal penemuan komputer, saat itu secara fisik komputer masih berbentuk bangunan ruang yang besar. Namun, dalam waktu beberapa tahun bentuk komputer telah mengecil, bahkan dapat saling berhubungan satu dengan yang lain. Hal tersebut merupakan sebuah lompatan teknologi manusia yang sangat luar biasa. Saat ini, dalam sebuah ruangan yang besar tidak lagi berisi satu komputer, akan tetapi telah berisi berpuluhan-puluhan, bahkan beratus-ratus komputer yang saling bersinergi membentuk sebuah *cluster* komputer yang mempunyai performa yang sangat andal dalam mengolah informasi.

Model komputer *single user* dan *stand alone*, yang dapat melakukan pekerjaan komputasi sendirian tanpa menyadari keberadaan komputer yang lain, akan tergantikan dengan era sistem komputerisasi yang saling terkoneksi dengan jumlah yang sangat banyak serta dapat saling berkomunikasi dan dapat saling berbagi pakai *resource* dalam menyelesaikan berbagai masalah informasi, meskipun dengan sistem operasi komputer yang berbeda-beda. Bukan suatu hal mustahil jika di masa mendatang, sistem operasi akan berada dalam sebuah sistem pelayan (*Server*) saja. Sebuah sistem operasi dapat dianggap sebagai udara bebas yang dapat diakses oleh siapa pun (*Client*), sehingga pertentangan antara sistem operasi yang bebas dengan sistem operasi *proprietary* tidak akan terjadi.

1.1 Jaringan

Kecepatan perkembangan teknologi menjadikan proses transformasi informasi sebagai kebutuhan utama manusia yang akan semakin mudah didapatkan dengan cakupan yang akan semakin luas. Perbedaan dalam hal pengumpulan, transportasi, penyimpanan serta pemrosesan informasi akan semakin hilang, sehingga akan tercipta sebuah sistem standar yang akan memudahkan manusia dalam mengembangkan teknologi sistem informasi.

Meleburnya sistem komputer dan komunikasi menjadikan perkembangan komunikasi jaringan semakin maju terutama pada perkembangan jaringan komputer. Menurut Tannenbaum (1981), jaringan komputer adalah *an interconnected collection of autonomous computers* (*suatu kumpulan interkoneksi dari komputer-komputer yang otonom*). Dua komputer dapat dikatakan saling terkoneksi dalam sebuah jaringan jika keduanya mempunyai kemampuan untuk saling berkomunikasi dan bertukar informasi. Media komunikasi tidak hanya melalui kabel, akan tetapi juga menggunakan media gelombang mikro, serat optik, hingga ke model wireless.

Jaringan komputer yang pertama adalah jaringan berdasarkan bagi pakai waktu atau *time-sharing network* menggunakan sebuah komputer pusat (*Mainframe*) serta beberapa terminal yang dihubungkan ke mainframe tersebut. Penerapan lingkungan jaringan seperti ini telah dilakukan oleh IBM dengan *System Network Architecture* (SNA) serta *Digital's Network Architecture*.

Perkembangan jaringan komputer selanjutnya mengikuti revolusi yang terjadi pada perkembangan PC. Produksi massal Personal Computer menjadikan kepemilikan perangkat ini semakin mudah dan murah. Local Area Network (LAN) berkembang mengiringi revolusi perkembangan PC. Kemampuan LAN semakin meningkat dalam melakukan pertukaran file dan pesan antarkomputer dalam area geografis yang relatif kecil. Komputer lain dapat melakukan bagi-pakai (*sharing*) resource serta bertindak sebagai penyedia atau server file.

Perkembangan tuntutan komunikasi dan sharing resource semakin diperlukan, sehingga diciptakan Wide Area Network (WAN) yang melakukan interkoneksi lintas LAN menggunakan jalur-jalur yang mendukungnya seperti media telepon maupun media interkoneksi lainnya. Sistem WAN tidak dibatasi oleh permasalahan geografis seperti pada sistem LAN.

Perkembangan jaringan saat ini telah mencapai pada kemampuan LAN dengan kecepatan tinggi dan teknologi switch antarjaringan yang semakin canggih. Aplikasi yang membutuhkan *high-bandwidth* semakin berkembang seperti aplikasi voice dan video conferencing dengan dukungan kecepatan tinggi.

Internetworking telah mampu memberikan solusi serta menjawab beberapa masalah antara lain terisolasi LAN, terjadinya duplikasi resource, dan ketiadaan pengaturan jaringan yang andal. Terisolasi LAN mengakibatkan komunikasi elektronis antara kantor atau departemen yang terkait tidak mungkin terjadi. Duplikasi resource berarti hardware dan software saling tumpang tindih dalam menyuplai informasi. Ketiadaan pengaturan jaringan berarti tidak ada metode terpusat yang menangani segala permasalahan jaringan.

1.2 Protokol

Apabila dua buah sistem saling berkomunikasi, hal pertama yang dibutuhkan adalah kesamaan bahasa yang digunakan, sehingga dapat memahami alur proses komunikasi. Lain halnya apabila dua buah sistem saling berkomunikasi dengan bahasa yang berlainan, tentunya dua sistem tersebut tidak akan saling memahami. Untuk itu, sistem tersebut membutuhkan sebuah mekanisme pengaturan bahasa yang dapat dipahami oleh dua buah sistem tersebut sehingga pertukaran informasi antarsistem akan dapat terjadi dengan benar. Aturan bahasa komunikasi ini sering disebut protokol komunikasi atau *communications protocols*. Protokol komunikasi merupakan aturan dalam melakukan pengiriman data (berupa blok-blok data) dari sebuah node jaringan ke node jaringan lain. Mekanisme pengaturan pertukaran data dalam jaringan komputer secara umum inilah yang akan dibahas dalam buku ini.

Beberapa definisi protokol adalah sebagai berikut:

When data is being transmitted between two or more devices something needs to govern the controls that keep this data intact. A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across wire) or high-level exchanges between application programs (e.g., the way in which two programs transfer a file across the Internet). [San Diego State University]

Ketika data ditransmisikan di antara dua atau lebih peralatan, diperlukan sesuatu yang dapat menjaga kontrol agar data tetap utuh, yaitu suatu deskripsi formal mengenai pesan dan aturan yang harus diikuti oleh dua

komputer yang ingin bertukar pesan. Protokol dapat mendeskripsikan detail dari interface mesin ke mesin level bawah (cara bagaimana dua program mentransfer file melalui Internet). [San Diego State University]

www.ichnet.org/glossary.htm

A protocol is a standardized means of communication among machines across a network. Protocols allow data to be taken apart for faster transmission, transmitted, and then reassembled at the destination in the correct order. The protocol used determines the way errors are checked, the type of compression, the way the sender indicates the end of the transmission, and the way the receiver indicates that the message has been received. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

Protokol merupakan sarana komunikasi antara mesin melalui jaringan yang terstandarisasi. Protokol mengizinkan data untuk ambil bagian dalam transmisi kilat, kemudian ditransmisikan, lalu dikumpulkan kembali sesuai arah dengan perintah yang benar. Protokol digunakan untuk mendeteksi kesalahan, tipe kompresi, dan bagaimana receiver (penerima) mengindikasikan bahwa pesan telah diterima. Protokol dapat mendeskripsikan detail level bawah dari interface machine to machine (misal bagaimana perintah bit dan byte dikirimkan melalui kabel) atau pertukaran level atas antara program alokasi (misal cara dua program mentransfer file melalui Internet).

www.cites.uiuc.edu/glossary/

A set of formal rules describing how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering and the transmission and error detection and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, the terminal-to-computer dialog, character sets, and sequencing of messages.

Seperangkat aturan formal yang mendeskripsikan cara mentransmisikan data, khususnya dalam jaringan. Protokol level bawah meliputi observasi terhadap standar elektrik dan fisik, perintah bit dan byte, pendekripsi-



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

A set of rules enabling computers or devices to exchange data with one another with as little error as possible. The rules govern issues, such as error checking and data compression methods. Also see communications protocol.

Seperangkat aturan yang memungkinkan komputer atau peralatan lain saling bertukar data dengan kesalahan sesedikit mungkin. Aturan tersebut meliputi cara mengecek kesalahan dan metode kompresi data. Lihat juga potokol komunikasi.

securityresponse.symantec.com/avcenter/refa.html

A computer protocol is a formal description of how computers talk to each other. Some common protocols include: TCP/IP (transmission control protocol/Internet protocol)--the standard piece of software that allows your computer to link up with SBC Yahoo!. POP (Post Office Protocol)--for accessing Internet e-mail. FTP (File Transfer Protocol)--for sending files from one computer to another over the Internet.

Protokol komputer merupakan deskripsi formal mengenai bagaimana komputer saling berhubungan. Protokol yang umum meliputi TCP/IP (Transmission Control Protocol/Internet Protocol), software standar yang mengizinkan komputer Anda untuk berhubungan dengan SBC Yahoo!; POP (Post Office Protocol), untuk mengakses e-mail di Internet; FTP (File Transfer Protocol), untuk mengirim file dari satu komputer ke komputer lain melalui Internet.

support.sbcglobal.net/general/662.shtml

A set of standardized rules for exchanging information among computers. Different protocols are used for different kinds of communication. For example, the HyperText Transfer Protocol specifies the rules for communication between World Wide Web servers and browsers. File Transfer Protocol sets the rules for copying files from one computer to another across a network.

Seperangkat aturan terstandarisasi untuk bertukar infomasi di antara komputer. Protokol yang berbeda digunakan untuk jenis komunikasi yang berbeda. Sebagai contoh, Hyper Text Transfer Protocol digunakan khusus untuk komunikasi antara server World Wide Web dan browser. File

Transfer Protocol digunakan untuk mengopi file dari komputer satu ke komputer lain dalam jaringan.

wings.avkids.com/SPIT/glossary.html

A set of standards used by two computers to communicate and exchange information with each other.

Seperangkat standar yang digunakan oleh dua komputer untuk berkomunikasi dan saling bertukar informasi.

www.wmo.ch/web/www/WDM/Guides/Internet-glossary.html

A set of formal rules describing how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering and the transmission and error detection and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, the terminal to computer dialogue, character sets, sequencing of messages etc.

Seperangkat aturan formal yang mendeskripsikan bagaimana cara men-transfer data, terutama dalam jaringan. Protokol level bawah meng-observasi standar elektrikal dan fisikal, perintah bit dan byte, pendekripsi transmisi dan kesalahan, serta koreksi terhadap aliran bit. Protokol level atas berkaitan dengan pemformatan data, meliputi sintaks pesan, terminal dari dialog komputer, susunan karakter, urutan pesan, dan lain-lain.

www.watchfire.com/products/webxm/glossary.asp

The set of formal rules that describe how to transmit data, especially across a network of computers.

Seperangkat aturan yang mendeskripsikan cara mentransmisikan data, khususnya saat melalui jaringan komputer.

www.lsoft.com/info/glossary.asp

This is the behavior and mutually determined set of formats and procedures that computers must follow in order to understand one another. In English, it is the set of rules governing the transfer of data and information between computers. If two computers do not use the same network protocol, then they cannot communicate. One example of a protocol is the TCP/IP suite.

Kebiasaan dan seperangkat format dan prosedur yang harus diikuti komputer untuk dapat saling memahami. Di Inggris, merupakan seperangkat aturan yang mengarahkan transfer data dan informasi antarkomputer. Jika dua komputer tidak menggunakan protokol jaringan yang sama, maka keduanya tidak dapat berkomunikasi. Contoh protokol adalah TCP/IP suite.

www.its.queensu.ca/network/overview/glossary.shtml

set of common rules (or language) that allow computers to communicate with each other. The standard protocol is TCP/IP (Transmission Control Protocol/Internet Protocol). The Web utilizes the HTTP protocol Server: any computer providing access to files, printing, communications and other services available to other users over a network.

Seperangkat aturan umum (atau bahasa) yang mengizinkan komputer-komputer untuk saling berkomunikasi. Protokol yang standar adalah TCP/IP (Transmission Control Protocol/Internet Protocol). Web menggunakan server protokol HTTP agar komputer dapat mengakses file, melakukan pencetakan, berkomunikasi, dan menyediakan layanan lain bagi user lain dalam jaringan.

www.idea-inc.org/glossary/index.php3

A standard for the exchange of information. Different computers and operating systems and software are able to communicate with each other on the Internet, because of the adoption of protocols.

Suatu standar pertukaran informasi. Komputer dengan sistem operasi dan software berbeda dapat saling berkomunikasi melalui Internet karena pengadopsian protokol.

www.walthowe.com/glossary/p.html

A set of formal rules and procedures which your computer must support in order to communicate with other computers on a network or through the Internet.

Seperangkat aturan dan prosedur formal yang digunakan komputer Anda untuk dapat berkomunikasi dengan komputer lain dalam jaringan atau melalui Internet.

iet.ucdavis.edu/glossary/

A set of rules governing the way in which two networked devices will communicate with each other. E.g. routers exchange routing information using the BGP protocol, at a more fundamental level all Internet devices exchange traffic using Internet Protocol.

Seperangkat aturan yang memuat cara bagaimana dua peralatan jaringan dapat saling berkomunikasi. Misalnya, router bertukar informasi routing menggunakan protokol BGP, atau pada level yang lebih fundamental, semua peralatan Internet bertukar trafik menggunakan Internet Protocol.

www.euro-ix.net/glossary/

A protocol is an algorithm, or step by step procedure, carried out by more than one party. Examples are network protocols, in which the steps are intended to ensure reliable transmission of information, or cryptographic protocols, in which the aim is to maintain some form of security relationship between the parties.

Protokol merupakan suatu algoritma atau prosedur langkah demi langkah, yang dihasilkan oleh lebih dari satu bagian. Misalnya, protokol jaringan, di mana langkah-langkah di dalamnya dimaksudkan untuk menjamin adanya transmisi informasi yang terpercaya, atau protokol kriptografik, yang bertujuan untuk mendapatkan beberapa bentuk hubungan keamanan antarbagian.

www.netcraft.com/ssl/glossary.html

A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information. A protocol is a standardized set of rules that specify how a conversation is to take place, including the format, timing, sequencing and/or error checking.

Suatu deskripsi formal dari pesan yang dipertukarkan dan aturan yang harus diikuti oleh dua atau lebih sistem yang bertukar informasi. Protokol merupakan standarisasi dari seperangkat aturan yang menentukan bagaimana suatu percakapan berlangsung, termasuk format, waktu, urutan, dan atau pemeriksaan kesalahan.

www.networkbuyersguide.com/search/105490.htm

In computer networks, a protocol is simply an agreed convention for inter-computer communication. Thus the TCP/IP protocol defines how messages are passed on the Internet, while the FTP protocol, which is built using the TCP/IP protocol, defines how FTP messages should be sent and received.

Dalam jaringan komputer, protokol merupakan konvensi yang disepakati untuk komunikasi antarkomputer. Selanjutnya, protokol TCP/IP mendefinisikan bagaimana pesan dikirimkan melalui Internet, sedangkan protokol FTP, yang dibangun menggunakan protokol TCP/IP, mendefinisikan bagaimana pesan-pesan FTP dikirim dan diterima.

www.utoronto.ca/ian/books/xhtml1/gloss/gloss.html

A set of formal rules or conventions governing the transmission, treatment, and formatting of data in an electronic communications system.

Seperangkat aturan formal atau konvensi yang menjadi tuntunan saat melakukan transmisi, memperlakukan, dan memformat data dalam sebuah sistem komunikasi elektronik.

https://www.namesecure.com/en_US/index.jhtml

In networking and communications, the specification that defines the procedures to follow when transmitting and receiving data. Protocols define the format, timing, sequence, and error checking systems used.

Dalam sistem jaringan dan komunikasi, ada spesifikasi prosedur yang harus diikuti saat akan mengirim atau menerima data. Protokol menentukan format, waktu, urutan, dan sistem pengecekan kesalahan yang digunakan.

www.angelfire.com/ny3/digi8tech/PGlossary.html

A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

Deskripsi formal dari format pesan dan aturan yang harus diikuti oleh dua komputer yang saling bertukar pesan. Protokol dapat mendeskripsikan detail level bawah dari interface machine to machine (misal, perintah bits dan byte yang dikirim melalui kabel) atau pertukaran level atas antara alokasi program (misal, cara dua program mentransfer file melalui Internet).

www.ncrel.org/tandl/k-12infra/k12infrad.htm

A standard set of rules that governs how computers or other electronics communicate with one another. Protocols define a message's format as well as how they are exchanged. Agreeing to a standard protocol allows different types of computer systems to communicate with one another in spite of their differences.

Aturan standar yang menuntun bagaimana komputer atau alat elektronik lain saling berkomunikasi. Protokol menangani bagaimana pesan terbentuk dan terkirim. Protokol standar mengizinkan sistem-sistem komputer dengan tipe berbeda untuk saling berkomunikasi dengan mengesampingkan perbedaan tersebut.

www.motorola.com/automotive/telematics/glossary/

A specific set of rules, procedures or conventions that two data devices must accept and use to be able to communicate. Protocols for data transmission cover such things as framing, error handling, transparency and line control.

Seperangkat aturan, prosedur, atau konvensi yang harus dipahami dan digunakan agar dapat berkomunikasi. Protokol untuk transmisi data meliputi pembuatan frame, penanganan eror, transparansi, dan kontrol baris.

www.rvcomp.com/wiring/EIA/glossary.htm

Set of well-defined rules that establish how entities on different computers or other network nodes interact. For example, the FTP protocol defines the rules and data formats used by FTP client software so that it can send or retrieve files from FTP server software executing on a different computer.

Sekumpulan aturan yang terorganisasi yang menyatakan bagaimana entitas dari komputer yang berbeda atau node jaringan lain berinteraksi. Misalnya, protokol FTP mendefinisikan aturan dan format data yang digunakan oleh software klien FTP, sehingga dapat mengirim atau memperoleh file dari software server FTP yang berasal dari komputer lain.

www.cddc.vt.edu/choices/1995/tutorial95.html

(computer science) rules determining the format and transmission of data

Aturan dalam ilmu komputer yang menentukan format dan transmisi data.

www.cogsci.princeton.edu/cgi-bin/webwn

Secara garis besar dapat disimpulkan bahwa protokol merupakan aturan standar, konvensi, format komunikasi, dan prosedur transmisi data.

1.3 Arsitektur Jaringan

International Standard Organization (ISO) telah mendefinisikan sebuah arsitektur jaringan yang disebut model referensi open systems interconnection. Dalam model OSI, peranan layering serta proses pertukaran data dalam sistem yang berlainan akan melalui sebuah hierarki atau tingkatan protokol komunikasi.

Model OSI terdiri dari tujuh layer, yaitu physical layer, data link layer, network layer, transport layer, session layer, presentation layer, dan application layer. Setiap layer berdiri sendiri dan terisolasi satu dengan yang lain. Hasilnya, dalam implementasinya hal tersebut justru lebih menyederhanakan proses pertukaran data. Perubahan dalam salah satu layer tidak akan memengaruhi layer yang lain. Oleh karena itu, desain layer ini sangat fleksibel dan dapat digunakan untuk mengakomodasi beberapa inovasi baik dari sisi teknologi hardware maupun firmware.

Selama tahun 1980-an hingga dekade ke depan, perhatian utama dalam interkoneksi jaringan masih menggunakan model referensi OSI karena model ini telah mengakomodasi beberapa fitur yang diperlukan untuk melakukan pertukaran data. Di samping itu, kemudahannya dalam melakukan koneksi secara universal membuat sistem menjadi model referensi yang digunakan hingga saat ini. Integrasi beberapa vendor yang



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

para vendor lelah menunggu kematangan protokol OSI. Protokol TCP/IP ternyata telah matang lebih dahulu dibanding model protokol OSI dengan memberikan layanan yang selama ini dijanjikan oleh protokol OSI, akan tetapi protokol OSI mempunyai variasi standar aplikasi yang lebih kaya dibandingkan protokol TCP/IP.

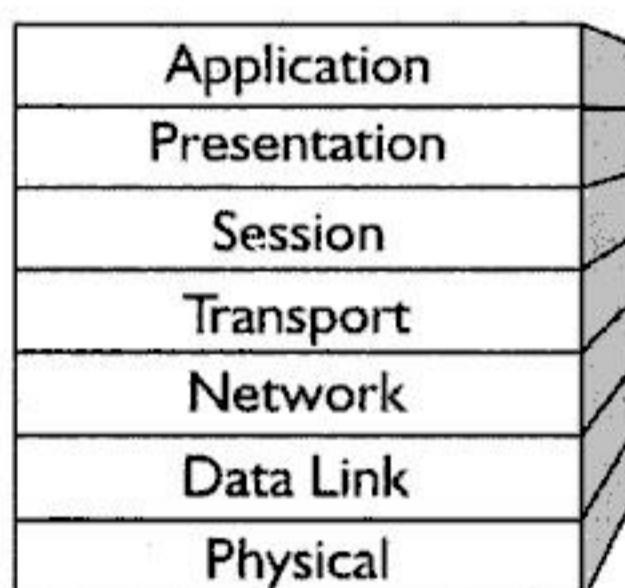
Terdapat tiga faktor yang membesarkan pertumbuhan TCP/IP, antara lain:

- ❖ Menjanjikan interoperabilitas. TCP/IP mempunyai protokol yang secara umum mendukung interoperabilitas produk-produk yang dihasilkan vendor-vendor yang berbeda. Vendor-vendor tersebut tidak hanya menggunakan TCP/IP, akan tetapi juga menggunakan jasa layanan aplikasi.
- ❖ Sangat menguntungkan dalam komersialisasi Internet. Saat ini, Internet telah dikuasai oleh protokol dengan base TCP/IP beserta layanan aplikasinya. Internet tumbuh sebagai media Information Superhighway. Berkembangnya keingintahuan masyarakat pengguna komputer secara umum dalam menggunakan Internet menjadikan protokol TCP/IP beserta layanannya dipercaya sebagai protokol yang powerful.
- ❖ Pertumbuhan perkakas pengelolaan jaringan. Manajemen protokol jaringan yang telah diimplementasikan secara luas adalah SNMP (*Simple Network Management Protocol*) yang menggunakan protokol TCP/IP. Beberapa produk vendor seperti hub, bridge, dan router telah menjadi agen SNMP.

1.3.2 Model Referensi Open Systems Interconnection (OSI)

Di depan telah disinggung tentang sebuah referensi model pertukaran data dalam jaringan yang menjadi acuan perkembangan jaringan secara umum, yaitu model Open Systems Interconnection (OSI). Referensi model OSI menggambarkan bagaimana informasi dari software aplikasi sebuah komputer berpindah melalui media jaringan ke software aplikasi komputer lain.

Model referensi OSI merupakan model konseptual yang terdiri dari tujuh layer, di mana setiap layernya mempunyai fungsi jaringan yang spesifik dan saling mendukung satu sama lain. Model ini telah dikembangkan oleh badan yang mengurus permasalahan standarisasi, yaitu International Organization for Standardization (IOS) di tahun 1984, dan hingga saat ini telah menjadi model arsitektur jaringan acuan dalam komunikasi antar-komputer. Model OSI membagi beberapa pekerjaan perpindahan informasi antara jaringan komputer ke dalam beberapa buah grup kecil yang lebih mudah diatur atau *manageable*. Setiap layer pada dasarnya dapat berdiri sendiri secara independen dalam implementasinya, akan tetapi tetap menyatu dalam fungsinya (berbeda-beda tetapi tetap satu fungsi yang saling mendukung). Dengan kemampuan ini, masing-masing layer dapat dikembangkan secara independen tanpa memengaruhi layer yang lain.



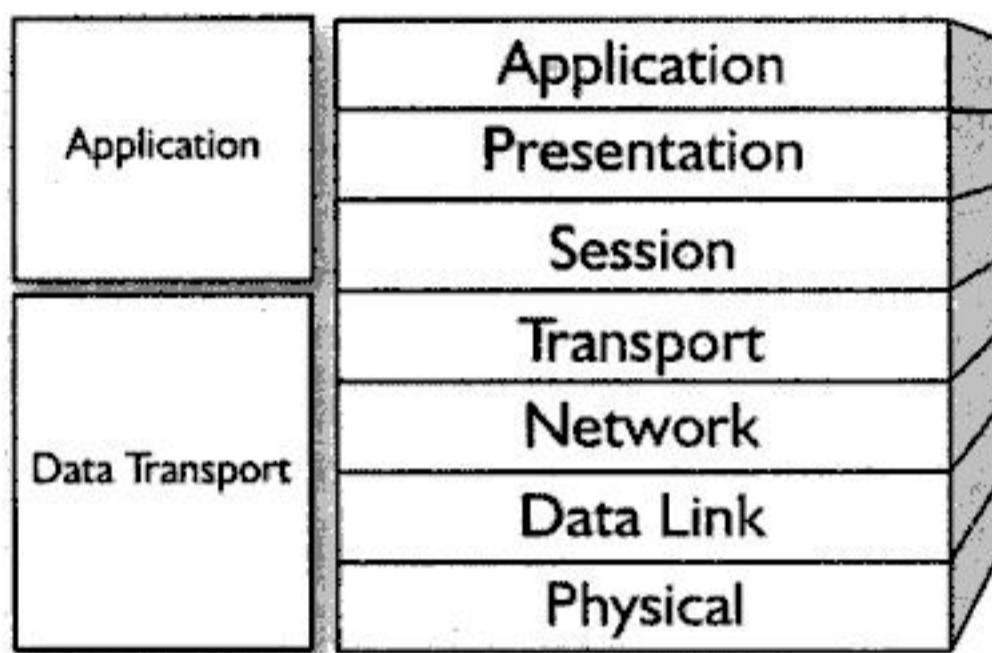
Gambar 1-2 OSI Layer

Ketujuh layer dari model referensi OSI dapat dibagi menjadi dua kategori utama, yaitu layer atas dan layer bawah.

Layer atas dari model OSI berkaitan dengan aplikasi dan implementasi secara umum sebuah software. Layer yang tertinggi, yaitu layer aplikasi, merupakan layer yang paling dekat dengan pengguna. Baik pengguna dan layer aplikasi melakukan proses interaksi menggunakan software yang berisi komponen komunikasi.

Layer di bawahnya berurusan dengan fungsi penanganan transportasi data. Layer physical dan data link diimplementasikan dalam hardware dan software. Layer bawah yang lain secara umum diimplementasikan

hanya dalam lingkungan software. Layer yang paling dekat dengan media jaringan adalah layer physical. Pengkabelan juga termasuk dalam layer ini, yang mempunyai tugas menempatkan informasi ke dalam media yang akan ditransmisikan ke seluruh jaringan.



Gambar 1-3 Dua Bagian OSI Layer

1.3.3 Layer Protokol

Begitu rumitnya pertukaran data antarjaringan, sehingga desain jaringan komputer harus disederhanakan dalam bentuk bagian-bagian tersendiri dalam sebuah lapisan-lapisan layer. Ide dasar dari desain jaringan yang terbagi dalam beberapa urutan layer adalah untuk mempermudah pemahaman, pengaturan, serta standarisasi pada setiap bagiannya.

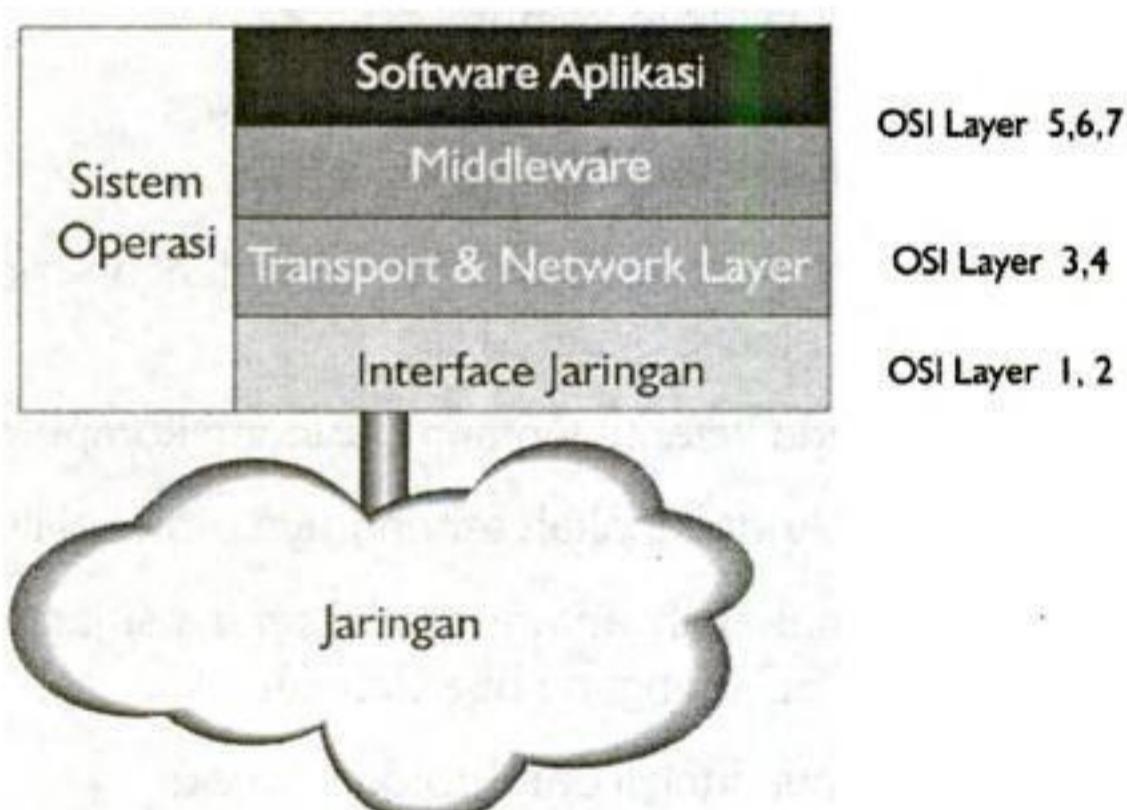
Jaringan komputer telah didesain dan dikonstruksikan dalam beberapa fungsional layer, dengan fungsi dan desain pada setiap layer yang berbeda. Setiap layer akan memberikan layanan ke layer di atasnya dan memberikan bungkus informasi untuk dapat diterapkan dan dipahami oleh layer di atasnya. Struktur aturan pertukaran informasi dan layanan pada setiap layer diatur dalam aturan tertentu, yaitu dalam sebuah arsitektur protokol jaringan.

Komunikasi antarnode jaringan berupa paket data harus didefinisikan dengan tepat, sehingga interpretasi ulang paket data dapat dilakukan dengan akurat, baik oleh sistem yang mengirimkan maupun sistem yang menerima paket data tersebut. Pertukaran paket antarnode jaringan akan diperantara oleh sebuah bahasa komunikasi atau disebut protokol.

Protokol ini mempunyai beberapa fungsi, antara lain penentuan jenis konektor, pengalaman titik-titik komunikasi, identifikasi interface, aturan-aturannya, pengaturan aliran data, menjaga ketersediaan data, laporan kesalahan, sinkronisasi, dan lain-lain. Pada praktiknya terdapat beberapa fungsi yang terangkum dalam sebuah kumpulan fungsi protokol atau suite/tumpukan protokol, di mana setiap protokol menangani satu aspek saja dalam proses komunikasi.

Protokol biasanya terstruktur bersama dalam sebuah bentuk desain layer, yang disebut tumpukan protokol atau *protocol stack*. Hampir semua arsitektur jaringan saat ini menggunakan dan dikembangkan dengan arsitektur layer protokol. Fungsi sesungguhnya dari setiap layer tersebut sangat bervariasi. Fungsi yang tegas biasanya dibedakan antara layer paling bawah dan layer di atasnya (lihat Gambar 1-3).

Layer bawah didesain untuk berurusan dengan ketersediaan koneksi atau memfasilitasi komunikasi dengan user. Layer ini menyembunyikan detail kerumitan fungsi pertukaran data secara fisik. Layer di atasnya (sering disebut middleware) bertanggung jawab terhadap konversi data pada apa yang disebut program aplikasi atau software. Secara fungsional terdapat layer yang bertugas untuk mengatur transportasi data. Layer ini bertanggung jawab terhadap koneksi antara layer atas (application oriented) dan layer bawah (network-oriented).



Gambar 1-4 Diagram Fungsional Protokol

Ide dasar arsitektur layer ini adalah membagi desain di atas menjadi bagian-bagian yang kecil. Setiap layer memberikan tambahan layanan yang telah disediakan oleh layer di bawahnya, sehingga dapat dikatakan bahwa layer yang paling atas akan menyediakan layanan yang lengkap untuk mengatur komunikasi dan menjalankan aplikasi yang terdistribusi. Prinsip dasarnya adalah kebebasan masing-masing layer dalam memberikan layanannya serta tidak perlunya pendefinisian layanan mereka terhadap layer lain di posisi atasnya. Dengan prinsip dasar ini, perubahan dalam sebuah layer tidak akan memengaruhi keseluruhan layer.

Pada awalnya tidak ada standarisasi pabrikan yang pasti antarpengembang dalam melakukan interkoneksi antarkomputer. Tidak adanya standarisasi menimbulkan tingginya beban biaya dalam menyelenggarakan komunikasi jaringan, karena tidak adanya standar yang baku. Masing-masing pabrikan mengembangkan produknya sendiri-sendiri dan tidak saling kompatibel. Akibatnya, proses ini justru memperumit masalah karena varian protokol banyak dibuat dan tidak semua varian mempunyai dokumen yang dipublikasikan.

Arsitektur Open Systems Interconnection (OSI) kemudian dikembangkan oleh International Organisation for Standardization (IOS) untuk memberikan jalan keluar secara operasional dan desain dari arsitektur layer-layer protokol jaringan. Model ini ternyata telah digunakan sebagai model bahasa referensi untuk melakukan komunikasi data.

1.4 Pertanyaan

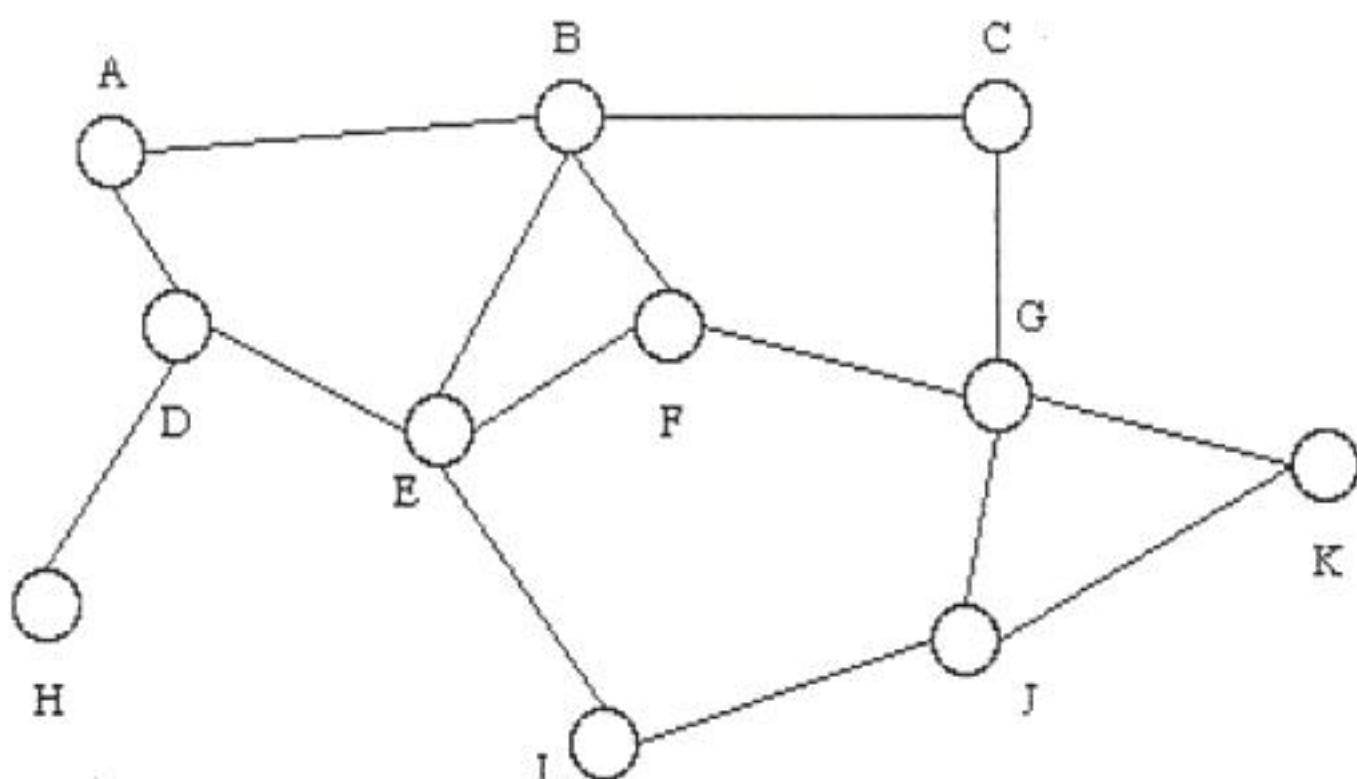
1. Apakah Hukum Moore masih relevan dengan pertumbuhan jumlah transistor hingga generasi saat ini?
2. Apakah yang Anda ketahui tentang clustering komputer?
3. Menurut definisi Anda, apakah sebenarnya protokol itu?
4. Lebih populer manakah antara model referensi jaringan TCP/IP dengan model OSI? Mengapa bisa demikian?
5. Apakah sebenarnya fungsi dari *Protocol Stack*?



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Koneksi antara user A dan D pada Gambar 2-1 direpresentasikan oleh beberapa seri link dari AB, BC dan CD, di mana setiap link terkoneksi dengan dua entitas atau node. Pada sirkuit point to point, setiap node menyediakan panel koneksi sederhana antara dua link atau sirkuit transmisi.

Saat user yang terkoneksi semakin banyak, ketersediaan sirkuit (*switching*) sudah tidak memungkinkan lagi untuk melakukan bagi pakai atau sharing. Untuk menanggulangi hal ini, jaringan komunikasi data dikembangkan lebih lanjut agar dapat dipergunakan untuk melakukan pertukaran informasi. Beberapa teknik switching antara lain switching sirkuit, switching message, dan switching paket. Setiap metode switching tersebut membutuhkan sharing fasilitas komunikasi antarpengguna (*end system*), dan setiap peralatan yang digunakan pada setiap node (*intermediate system*) dipakai untuk mengganti panel koneksi pada metode point to point. Akhirnya jaringan akan terbentuk menjadi bermacam-macam link, yang terdiri atas beberapa jalur. Komunikasi data dalam jaringan tersebut harus dapat menyeleksi jalur yang tepat pada koneksi yang dibutuhkan.

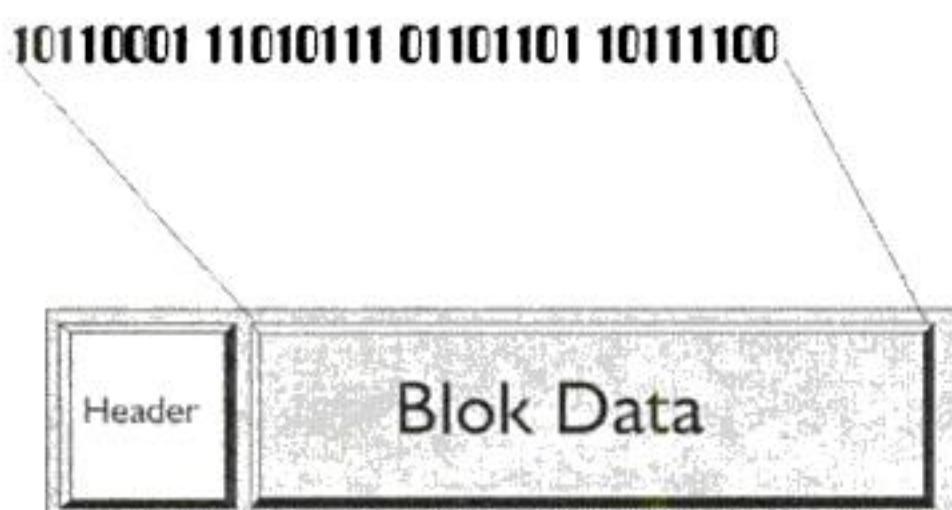


Gambar 2-2 Jaringan yang Relatif Kompleks dari Node A – K

Terdapat tiga pendekatan untuk menghasilkan waktu jeda yang minimum, yaitu menggunakan switching sirkuit, switching message, dan switching paket. Performa switching tersebut tergantung pada kekuatan, kecepatan, dan nilai koneksi yang tersedia.

2.1 Protokol Komunikasi

Setelah memahami sirkuit komunikasi, hal yang penting dalam sebuah jaringan adalah aturan pertukaran data atau protokol komunikasinya. Data dapat Anda bayangkan sebagai informasi satu dimensi dari bit-bit sinyal digital yang membentuk pola tertentu dan dipahami sebagai kode bahasa mesin komputer. Data tersebut akan disegmentasikan dalam beberapa bagian yang membentuk suatu blok data.

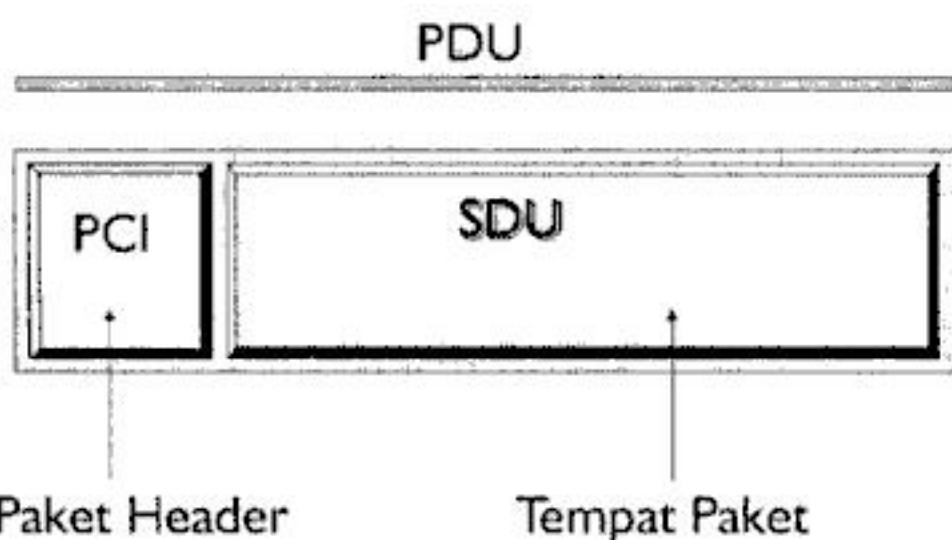


Gambar 2-3 Bentuk Satu Dimensi Data Diinterpretasikan Sebagai Blok

Protokol komunikasi mendefinisikan aturan-aturan dalam mengirim blok-blok data dari satu node jaringan ke node yang lain. Satu blok data disebut Protocol Data Unit (PDU).

Protokol biasanya didefinisikan dalam tingkatan-tingkatan layer (dengan referensi model OSI) yang telah dibahas pada bab sebelumnya. Spesifikasi protokol terdiri dari operasional protokol serta bagaimana implementasinya. Spesifikasi protokol terdiri dari tiga paket antara lain:

- Definisi dari format Protocol Control Information (PCI) menggunakan bentuk PDU Header.
- Definisi prosedur untuk transmisi dan menerima Protocol Data Unit (PDU).
- Definisi layanan yang disediakan oleh layer protokol.



Gambar 2-4 Protocol Data Unit

Pertukaran data pada PDU terbagi menjadi dua bagian, yaitu header (PCI) dan Service Data Unit (SDU). Protokol tidak untuk mendefinisikan atau memaksa bagian data untuk ditempatkan di SDU, akan tetapi hanya berisi format di PCI yang digunakan untuk mendefinisikan field serta bagaimana caranya agar pola-bit tersebut dapat diinterpretasikan.

Protokol juga mendefinisikan prosedur yang digunakan untuk menentukan bagaimana PDU dapat diproses saat ditransmisikan serta diterima pada node yang menerimanya. Prosedur ini akan menentukan nilai valid dari field PCI, dan suatu tindakan akan dilakukan pada saat penerimaan nilai PCI yang didasarkan pada informasi kontrol yang telah tersimpan. Prosedur-prosedur yang diterapkan dalam sebuah protokol meliputi:

- ❖ Recovery dari terjadinya kesalahan (Prosedur checkpoint dan prosedur go-back-n)
- ❖ Pengaturan aliran data
- ❖ Segmentasi
- ❖ Pemilihan layanan access point
- ❖ Manajemen koneksi

Protokol biasanya diimplementasikan dengan cara menuliskan sejumlah program atau proses yang akan berkomunikasi ke pihak lain menggunakan antrean dan pemanggilan fungsi. Untuk memastikan operasi dari protokol tersebut, biasanya membutuhkan satu atau lebih timer atau pewaktu. Untuk menjalankan atau menghentikan timer, protokol biasanya menggunakan interface sistem operasi pada komputer tersebut. Interface ini juga digunakan untuk meminta atau me-request buffer kosong untuk



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Kita akan lebih mudah memahami pemaketan data jika menggunakan analogi pengiriman surat. Surat merupakan paket data yang telah siap dikirimkan atau dapat dikatakan bahwa proses pemaketan beberapa unsur seperti kertas, amplop, dan perangko merupakan sebuah Protocol Data Unit. Kertas merupakan tempat data atau Service Data Unit-nya, yang tentunya harus diberi alamat tujuan. Untuk memudahkan pendataan, beberapa informasi (Protocol Control Information/PCI) seperti alamat tujuan, identitas pengirim, jenis surat yang dikirimkan, serta berbagai tambahan-tambahan informasi yang lain, akan dituliskan di dalam amplop.

Gambar 2-5 merupakan contoh model referensi OSI yang mendukung komunikasi peer to peer antara dua buah End System (ES). Pada kasus tersebut, entitas dari protokol transport akan berkomunikasi secara end to end menggunakan layanan jaringan layer di bawahnya. Komunikasi peer to peer antar-end system akan digantikan oleh protokol komunikasi.

Pada layer data link, komunikasi akan saling bertukar menggunakan layanan physical layer. Komunikasi akan terjadi pada bagian protokol layer data link yang kemudian akan mengoneksikan sistem tersebut, baik Intermediate System atau End System.

Pada kenyataannya, tidak ada data yang secara langsung berhubungan dari layer $N+1$ sistem mesin satu ke layer $N+1$ sistem mesin yang lain, kecuali pada layer paling bawah yaitu layer N. Setiap layer hanya akan mengontrol informasi, kemudian melewatkannya dengan segera ke layer di bawahnya. Saat sudah mencapai layer paling bawah, data baru dapat ditransformasi ke sistem lain. Pada layer paling bawah akan terjadi komunikasi secara fisik dengan sistem mesin yang lain, sedangkan pada layer di atasnya hanya terjadi komunikasi virtual. Pada Gambar 2-5 terlihat bahwa layer $N+1$ akan saling berhubungan dengan layer yang sejenis melalui komunikasi virtual.

Pada dasarnya, setiap antarpasangan layer yang berdekatan mempunyai sebuah layanan interface. Interface ini akan mendefinisikan operasi dasar dan layanan dari layer paling bawah ke layer di atasnya.

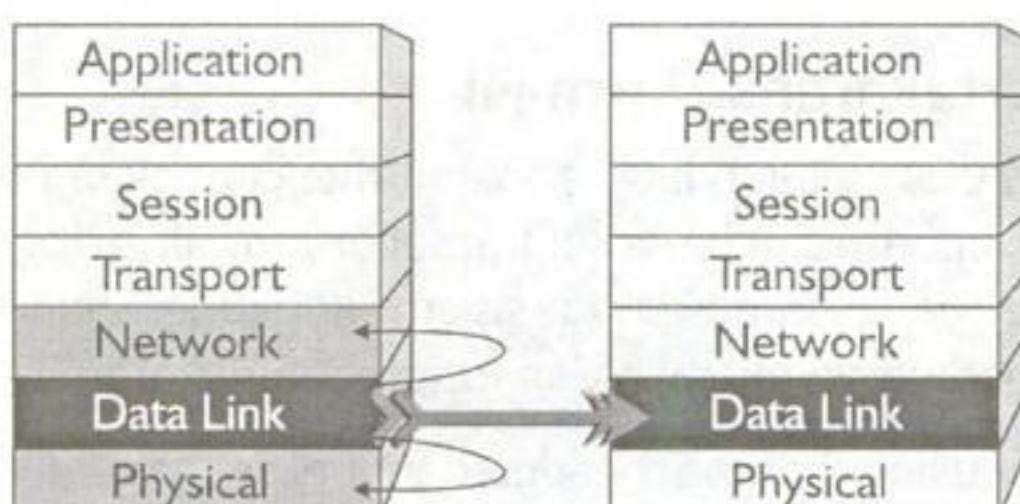
2.3 Komunikasi Antarsistem Model OSI

Informasi akan ditransfer dari software aplikasi sebuah sistem komputer ke aplikasi sistem lainnya melewati setiap layer pada model OSI. Sebagai contoh, aplikasi software di sistem A mempunyai informasi yang akan ditransmisikan ke aplikasi software sistem B, sehingga program aplikasi di sistem A akan melewatkkan informasi ke layer aplikasi (Layer 7) di sistem A tersebut. Selanjutnya, layer aplikasi akan melanjutkan informasi tersebut ke layer di bawahnya, yaitu layer presentasi (Layer 6), kemudian melakukan relay data ke layer session (Layer 5) hingga menuju ke layer fisikal (Layer 1).

Pada layer fisikal, informasi akan ditempatkan pada media jaringan fisik kemudian dikirimkan melintasi media jaringan ke sistem B. Layer fisikal akan memindahkan informasi dari media fisik ke layer data link (Layer 2), yang juga dilewatkan ke layer network (Layer 3), dan seterusnya hingga mencapai layer aplikasi (Layer 7) pada sistem B. Selanjutnya, layer aplikasi sistem B akan menampilkan informasi pada program aplikasi penerima, sehingga selesailah proses komunikasi tersebut.

2.3.1 Interaksi Antarlayer

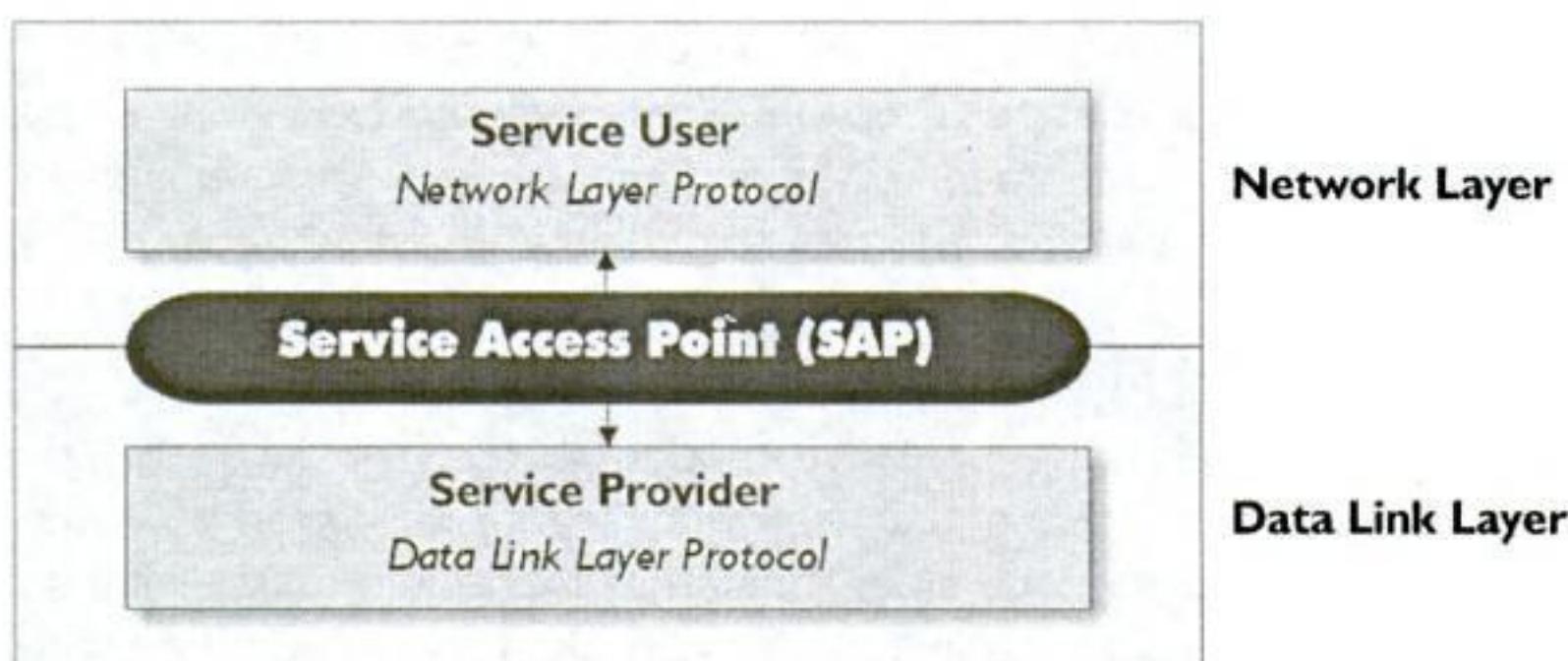
Secara umum, sebuah layer dalam model OSI akan melakukan proses komunikasi dengan 3 layer yang lain, yaitu layer di atasnya, di bawahnya, dan layer yang sama pada sistem tujuan di mana informasi dikirimkan. Sebagai contoh, layer data link di sistem A akan melakukan komunikasi dengan layer network dan layer fisiknya serta berkomunikasi dengan data link di sistem B.



Gambar 2-6 Interaksi Antarlayer pada Model OSI

Salah satu layer akan berkomunikasi satu dengan yang lain menggunakan layanan yang telah disediakan pada layer kedua. Layanan yang disediakan oleh layer terdekatnya akan membantu komunikasi dengan layer pada sistem komputer lain. Tiga elemen dasar yang ada pada layanan layer tersebut adalah service user, service provider, dan service access point (SAP). Pada konteks ini, service user pada layer OSI adalah permintaan layanan dari layer OSI terdekat.

Service provider adalah layer OSI yang menyediakan layanan untuk melayani service user. Layer OSI dapat menyediakan layanan untuk beberapa service user. SAP merupakan lokasi konseptual di mana salah satu layer OSI dapat meminta layanan ke layer OSI yang lain. Untuk memahami pertukaran data dan interaksi antarlayer dapat dilihat pada Gambar 2-7



Gambar 2-7 Interaksi pada Network dan Data Link Layer

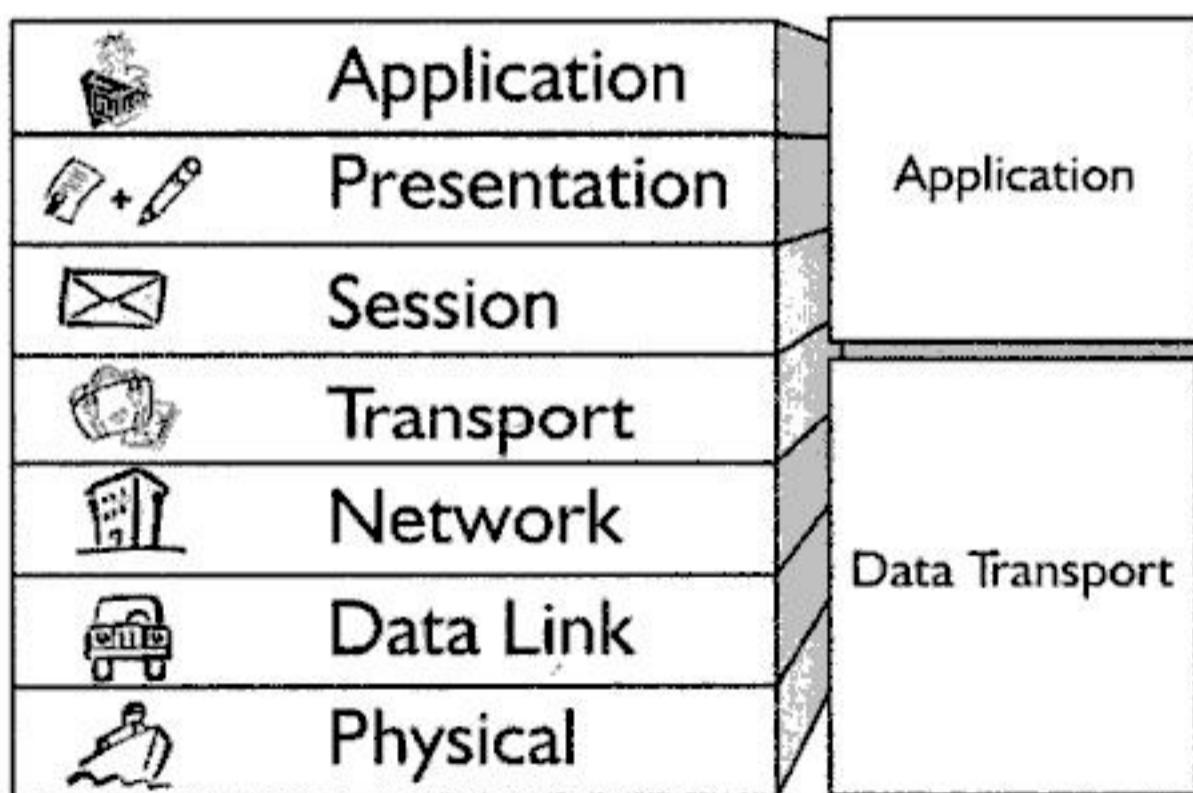
2.3.2 Pertukaran Informasi

Dalam model OSI, ketujuh layer tersebut menggunakan beberapa bentuk pengontrolan informasi (Control Information) untuk saling berkomunikasi dengan layer yang sama pada sistem komputer yang lain. Control Information berupa permintaan dan instruksi pertukaran data antarlayer.

Control Information berupa header dan trailer, atau dapat diibaratkan sebagai kepala dan rangkaian yang mengikutinya. Header dan trailer akan selalu disertakan pada setiap layer di bawahnya, atau sering disebut

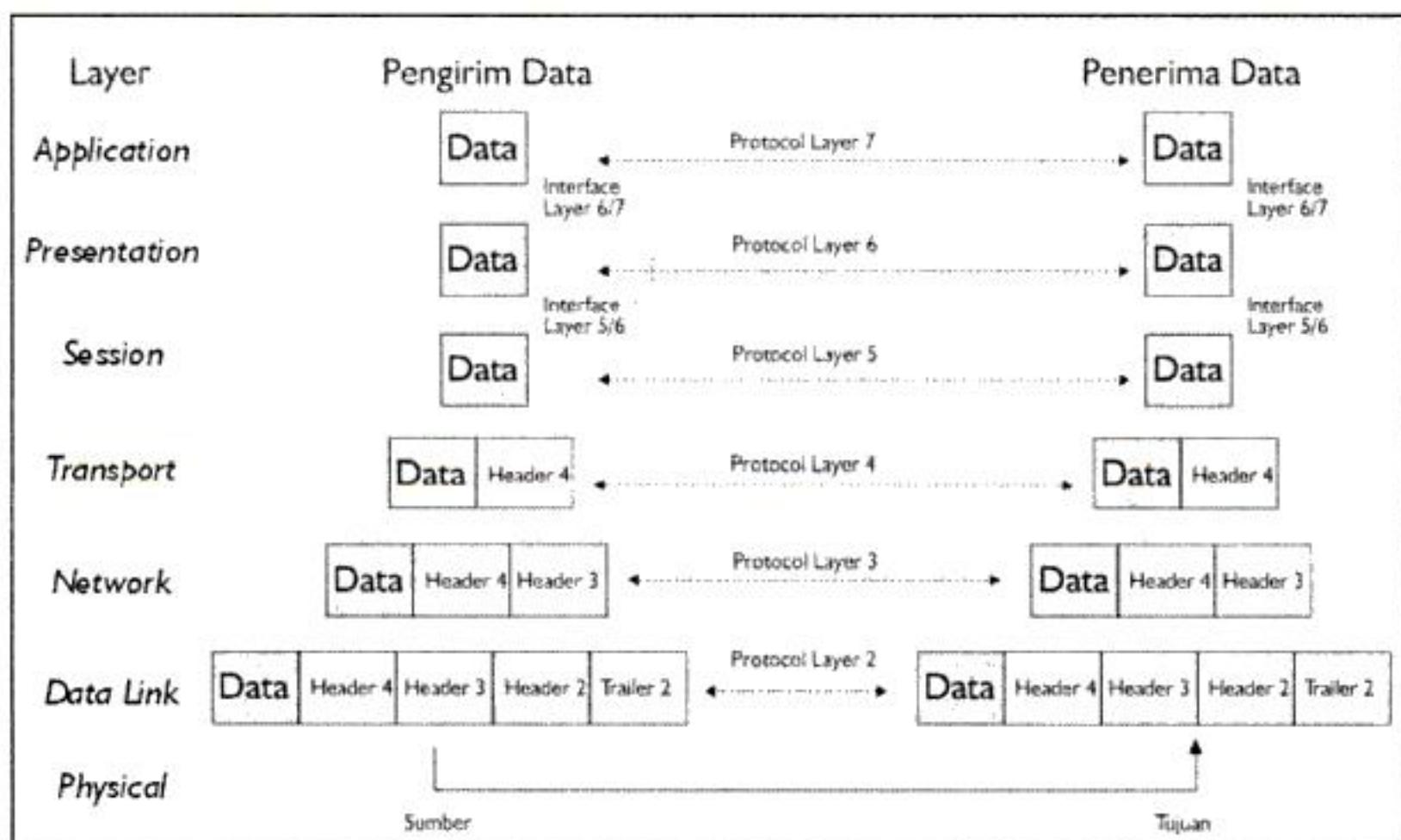
pengkapsulan atau *encapsulated*. Penjelasan mengenai *encapsulated* dapat dianalogikan dengan surat, seperti disinggung pada pembahasan sebelumnya (Gambar 2-8). Surat terdiri dari selembar kertas atau lebih, yang berisi tulisan dengan format tertentu untuk mempermudah menjelaskan kepada siapa surat tersebut ditujukan. Lembaran kertas tersebut tidak mungkin langsung dikirimkan apabila tidak dibungkus terlebih dahulu dengan amplop yang akan dilabeli perangko dan ditulisi alamat tujuan dan si pengirim. Proses penambahan amplop dan perangko serta alamat tujuan dan pengirim inilah yang dinamakan proses *encapsulated data*. Setelah amplop yang berisi surat siap dikirimkan, selanjutnya amplop dapat dimasukkan di bis surat atau langsung dibawa ke kantor pos. Di kantor pos, surat akan dikelompokkan sesuai alamat tujuan, kemudian dibungkus kembali dengan bungkus yang lebih besar untuk mempermudah pengangkutan, satu bungkus untuk satu daerah tujuan.

Proses amplop, pembungkusan, pengepakan, dan pengangkutan merupakan proses penambahan header dan trailer pada tingkatan layer di posisi bawah layer berikutnya hingga ke layer paling bawah (fisik). Proses pengepakan dan penambahan bungkus tidak mungkin dilakukan pada layer-layer di atasnya sebab semakin ke atas, bungkus tersebut akan dibuka dan dibuang untuk mengambil informasi di dalamnya yang memang dibutuhkan oleh layer yang semakin ke atas.



Gambar 2-8 Analogi Encapsulated Data

Masing-masing layer tersebut akan saling berkomunikasi secara virtual melalui protokol dalam bahasa dan layer yang sama. Data hanya akan dikomunikasikan melalui kontak fisik layer yang paling bawah. Hal yang paling penting adalah relasi antara komunikasi virtual dan komunikasi aktual serta perbedaan antara protokol dan interfacenya. Diagram pertukaran data pada Gambar 2-9 akan lebih memperjelas mekanisme pertukaran data, baik yang melibatkan komunikasi virtual serta aktual maupun perbedaan protokol dan interfacenya.



Gambar 2-9 Informasi Aktual dan Komunikasi Virtual

Dari gambar di atas terlihat bahwa data akan dihasilkan dari layer 7. Data tersebut akan dikirimkan ke layer bawahnya melalui interface, hingga layer 4. Selanjutnya, layer 4 akan memecah data tersebut dalam unit-unit yang lebih kecil untuk mempermudah proses transformasi data, di mana setiap unit data akan diberikan sebuah *header*. Header ini berisi informasi pengatur, misal jumlah unit dan urutannya, sehingga penerima akan dapat menyusun kembali data unit tersebut berdasarkan informasi header. Setiap melalui layer di bawahnya akan ditambahkan header informasi untuk tujuan yang sama hingga pada layer 2. Untuk mempersiapkan transformasi data melalui jalur fisik (informasi aktual) akan ditambahkan trailer, yaitu media pengangkut yang akan dialirkan melalui transmisi media fisik.

2.4 Arsitektur Jaringan Wireless

Arsitektur jaringan komputer terdiri dari protokol dan komponen yang dibutuhkan dalam menjalankan sebuah aplikasi. Salah satu standar jaringan yang telah dibahas pada bagian depan buku ini adalah arsitektur model referensi dari Open System Interconnect atau OSI. Standarisasi model referensi OSI juga sangat berguna dalam menggambarkan beberapa standar jaringan serta interoperabilitasnya termasuk dalam jaringan wireless.

Secara garis besar, fungsional ketujuh layer model referensi OSI adalah:

Layer 1 – Physical Layer. Layer ini secara fisik terkoneksi satu dengan yang lain dan menyediakan transmisi aktual dari informasi melalui media, baik wired maupun wireless. Layer ini merupakan aliran dari bit (binary digit 1 dan 0) berupa denyut elektris, sinyal radio, atau sinar cahaya yang melalui jaringan pada level elektrikal dan mekanikal. Layer ini merupakan layer secara hardware yang bertugas untuk mengirim dan menerima data pada sisi pembawa (carrier) termasuk pengkabelan, kartu, bentuk port koneksi, serta aspek fisik lainnya.

Layer 2 – Data Link Layer. Pada layer ini paket-paket data akan dienkode dan didekode menjadi susunan bit-bit. Data tersebut dipecah menjadi frame-frame data, kemudian ditransmisikan dan diurutkan. Selanjutnya, pengaturan sinkronisasi frame akan diproses jika terjadi kesalahan baik pada pengirim maupun penerima. Layer data link terbagi menjadi dua sublayer, yaitu Media Access Control (MAC) dan Logical Link Control (LLC). Sublayer MAC akan mengatur bagaimana komputer di jaringan mendapatkan akses data serta permission-nya untuk kemudian melakukan proses transmisi. Sublayer LLC akan mengatur sinkronisasi layer, aliran data, dan melakukan pemeriksaan apabila terjadi kesalahan. Jaringan wireless biasanya menyertakan koordinasi akses melalui media udara dan bagaimana proses recovery apabila terjadi kesalahan saat perambatan data dari pengirim maupun penerima data.

Layer 3 – Network. Layer ini menyediakan proses penentuan rute paket di jaringan dari pengirim ke penerima. Layer ini juga menyediakan beberapa teknologi untuk melakukan switching dan routing, membuat path secara logika yang disebut sirkuit virtual, dan melakukan transmisi

data dari node ke node. Proses routing berguna untuk memastikan bahwa paket data tersebut terkirim pada arah yang benar untuk tujuan tertentu. Protokol seperti Internet Protocol (IP) beroperasi pada layer ini. Selain proses routing, proses yang dilakukan oleh layer ini adalah proses forwarding, metode pengalaman, internetworking, penanganan kesalahan, mengontrol tabrakan data, dan proses pengurutan paket.

Layer 4 – Transport. Layer ini juga disebut layer host to host atau end to end, artinya layer ini menyediakan proses transfer data secara transparan antar-end system (host) serta bertanggung jawab terhadap metode recovery kesalahan end to end. Layer ini juga mempunyai fungsi sebagai pengatur aliran data serta selalu memastikan kelengkapan data saat dilakukan proses transfer. Contoh protokol yang beroperasi pada layer ini adalah Transmision Control Protocol (TCP).

Layer 5 – Session. Layer ini berfungsi untuk membentuk, mengatur, dan menghentikan koneksi antaraplikasi. Layer ini akan mengatur koordinasi, menghentikan percakapan antarsistem, pertukaran data, dan dialog antaraplikasi. Pada model wireless middleware, sebuah pengatur akses akan bertugas menyediakan bentuk konektivitas pada jaringan wireless tersebut. Jika terjadi interferensi pada jaringan wireless, layer ini akan melakukan penundaan komunikasi hingga interferensi tersebut hilang.

Layer 6 – Presentation Layer. Layer ini bertugas melakukan negosiasi sintaks-sintaks transfer data untuk layer aplikasi dan berfungsi sebagai penerjemah di antara data format yang berlainan. Layer ini akan melakukan translasi serta proses pengkodean untuk mewakili data saat berkomunikasi pada sistem yang dikembangkan oleh vendor yang berlainan, sehingga layer dan enkripsi data akan dikirimkan melintas jaringan tanpa harus selalu mempertimbangkan permasalahan kompatibilitas.

Layer 7 – Application Layer. Layer ini menyediakan komunikasi antara user dengan layanan komunikasi standar seperti transfer dan e-mail. Beberapa software yang berjalan di atas layer ini adalah Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), dan File Transfer Protocol (FTP).

Kombinasi layer pada arsitektur jaringan di atas mendefinisikan fungsionalitas yang sama pada jaringan wireless. Akan tetapi, jaringan



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

memberikan pandangan apakah data dapat dikirimkan dari satu titik ke titik yang lain, dan akan mengidentifikasi jumlah bandwidth efektif pada media, sehingga dapat menyuplai dan mendukung keberadaan sinyal digital.

Data rate sebuah sinyal adalah total jumlah bit yang ditransmisikan berhubungan dengan waktu yang diperlukan untuk melakukan pengiriman. Unit umum yang digunakan untuk mengukur bit rate adalah bits per second (bps). Sebagai contoh, dalam satu detik terdapat 1.000.000 sinyal, sehingga data rate sinyal adalah 1.000.000 dibagi satu detik sama dengan 1.000.000 bit per detik atau 1Mbps.

Troughput. Pada dasarnya throughput sama dengan data rate, akan tetapi secara umum perhitungan throughput meniadakan bit-bit tambahan (overhead) yang dimasukkan pada saat komunikasi terjadi. Tidak ada standar untuk menampilkan throughput, tetapi biasanya throughput merupakan informasi aktual yang dikirimkan melalui jaringan. Throughput memberikan akurasi dalam representasi performa dan efisiensi jaringan terutama pada jaringan wireless. Semakin tinggi throughput, akan semakin baik performa jaringan. Throughput dapat dikatakan sebagai perbandingan persentase antara input dan output data pada jaringan wireless.

Overhead dalam data ini biasanya berupa header pada setiap frame, field-field yang berisi kontrol kesalahan, frame pengenal, dan transmisi ulang karena terjadi kesalahan. Akibatnya, informasi menjadi terbebani dan trafik akan melambat. Jika dalam sebuah jaringan mempunyai data rate 11 Mbps, tetapi throughput aktual sinyal digitalnya hanya berkisar setengahnya atau sekitar 5 Mbps, maka overhead akan diabaikan.

2.4.2 Udara Sebagai Media Pertukaran Data

Pada jaringan wireless, media yang digunakan sebagai antarmuka atau interface adalah media udara. Saat peralatan komputer akan mengirimkan informasi melalui jaringan wireless, langkah pertama yang dilakukan adalah melakukan negosiasi koneksi terhadap komputer remote-nya menggunakan fungsi-fungsi di layer transport dan session. Setelah komputer mendapatkan koneksi, peralatan komputer akan mengirimkan data dalam bentuk digital ke NIC (Network Interface Card) wireless. Selanjutnya, NIC wireless akan mengirimkan frame yang berisi informasi

penyesuaian pada standar tertentu, seperti standar IEEE 802.11 (akan dibahas pada bab selanjutnya) ke remote komputer atau pada access point.

NIC wireless akan mengirimkan data dan mengonversinya menjadi frekuensi radio analog sebelum mentransmisikan data melalui antena. Media ini tidak mengenal informasi dalam bentuk digital karena pengiriman data dilakukan melalui media udara. Konversi ini akan mengakibatkan terjadinya modulasi. Setelah terjadi modulasi, sinyal akan merambat melalui media udara dan akan diterima oleh NIC wireless tujuan. Proses selanjutnya adalah proses demodulasi, yaitu proses penerimaan data untuk selanjutnya dimanipulasi agar informasinya dapat digunakan pada layer-layer selanjutnya.

2.5 Pertanyaan

1. Apa yang Anda ketahui tentang konsep sharing?
2. Apabila user jaringan bertambah banyak, apakah konsep sharing tersebut masih dapat digunakan?
3. Apakah yang Anda ketahui tentang Protocol Data Unit (PDU)?
4. Bagaimana prosedur yang diterapkan pada setiap protokol?
5. Apa yang Anda ketahui tentang komunikasi peer to peer?
6. Apa yang Anda ketahui tentang encapsulated data?
7. Jelaskan apa yang disebut komunikasi virtual dan komunikasi aktual!
8. Apakah fungsi header dan trailer, dan mengapa harus diberi header?
9. Apa yang Anda ketahui tentang MAC dan LLC ?



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

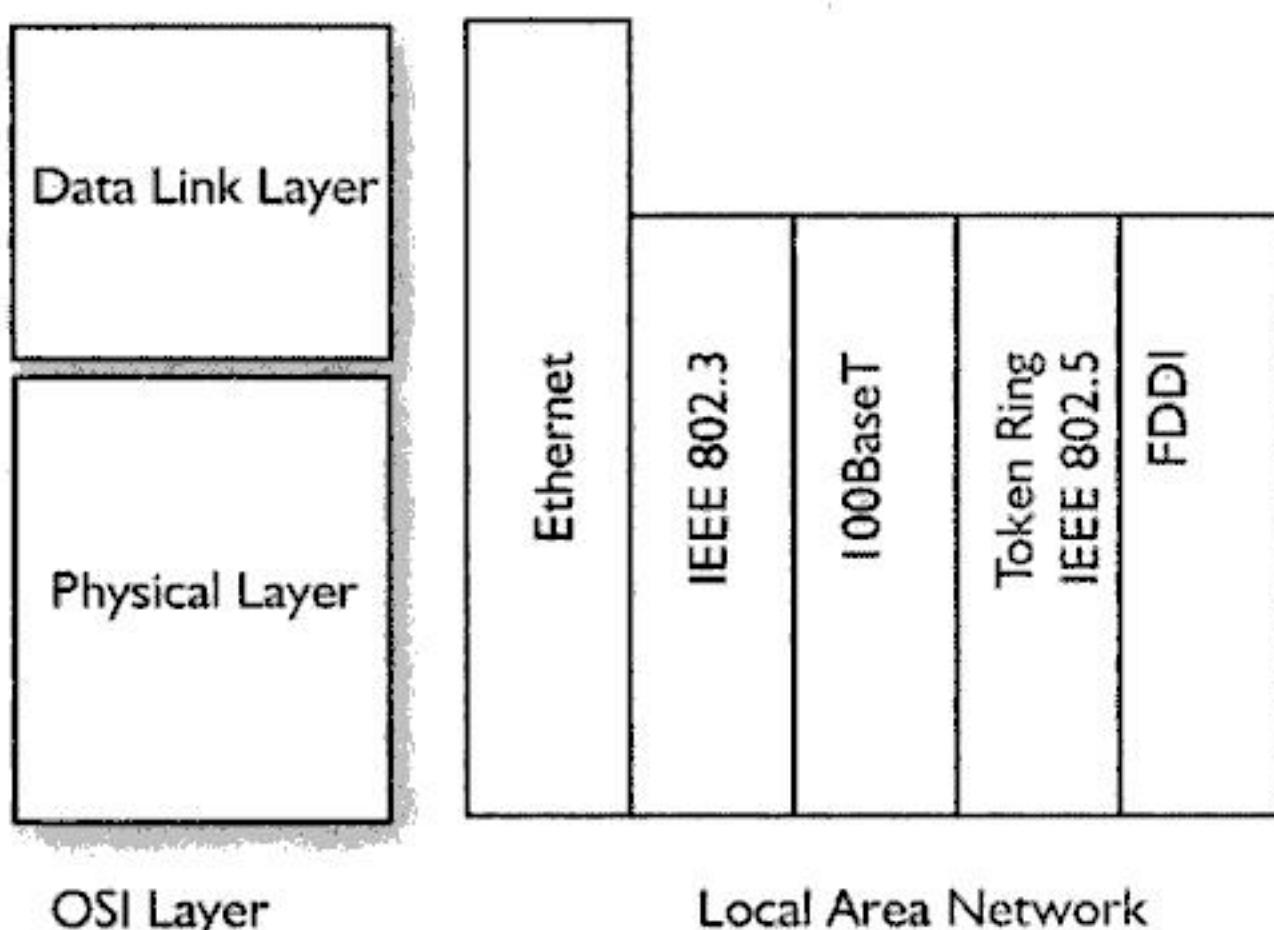


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

kembang, seperti aplikasi multimedia, voice dan video conferencing. Implementasi jaringan pada layer fisik dapat berupa spesifikasi untuk LAN maupun WAN.

3.1.2 Protokol LAN

Protokol LAN mempunyai beragam metode media dalam melakukan akses, metode transmisi, topologi, dan peralatannya. Peralatan-peralatan LAN dapat dilihat pada Gambar 3-1, antara lain Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, dan Fiber Distributed Data Interface (FDDI).



Gambar 3-1 Implementasi Layer Fisik pada Spesifikasi LAN

LAN mempunyai fitur-fitur andal, antara lain kecepatan tinggi dan toleransi terhadap kesalahan data yang baik dalam cakupan wilayah geografi yang relatif kecil. Secara spesifik, jaringan ini melakukan koneksi antara beberapa workstation, personal computer (PC), printer, dan peralatan lain dalam satu kawasan yang relatif kecil. LAN menawarkan keuntungan kepada pengguna, antara lain dapat melakukan bagi pakai terhadap peralatan dan aplikasi, pertukaran file yang intensif di antara peralatan yang saling terkoneksi, serta fitur aplikasi komunikasi menggunakan electronic mail serta aplikasi-aplikasi yang lain.

3.1.3 Peralatan pada Layer Fisik

Pada layer fisik, sangat penting bagi Anda untuk memahami bermacam-macam peralatan LAN dan cara kerjanya. Perbedaan utama antara jaringan wired dan wireless adalah pada peralatan-peralatan fisik yang saling terkoneksi dan saling berkomunikasi. Beberapa peralatan tersebut beroperasi pada model layer fisik OSI, yang dapat memanipulasi aliran data jaringan dalam aspek fisik (seperti tegangan, arah sinyal, dan kekuatan sinyal). Beberapa peralatan yang sangat umum digunakan pada layer ini adalah:

Network Interface Card (NIC), merupakan komponen yang menyediakan koneksi antarbus internal komputer dengan media jaringan. NIC sering disebut kartu jaringan yang mempunyai model dan bentuk yang semakin beragam.

Transciever, merupakan bagian dari interface jaringan yang melakukan pengiriman dan penerimaan sinyal pada jaringan (transmitter/receiver). Setiap interface jaringan merupakan sebuah transciever. Beberapa NIC mempunyai bentuk port konektor yang berbeda-beda atau Attachment Unit Interface (AUI), sehingga dibutuhkan transciever eksternal untuk melakukan koneksi dengan media NIC yang berlainan bentuk.

Repeater, merupakan peralatan di layer fisik yang mempunyai fungsi sebagai penguat sinyal, yaitu saat akan dilakukan proses pengiriman ulang (resend) sinyal dalam sebuah port. Repeater berguna untuk memperpanjang jarak maksimum segmen jaringan, biasanya diletakkan pada station jaringan yang jauh dari keseluruhan jaringan utama.

Hub, merupakan peralatan yang sangat umum dan populer digunakan setelah NIC, yaitu sebuah repeater yang mempunyai banyak port. Fungsi hub adalah melakukan pengulangan pesan dari port satu ke port yang lain. Hub terdiri dari dua jenis, yaitu:

- ❖ Hub aktif, menggunakan catu daya untuk memperkuat sinyal dan sangat efektif untuk menangani keterbatasan panjang segmen jaringan.
- ❖ Hub pasif, tanpa menggunakan catu daya sehingga praktis hanya berupa sambungan fisik dan koneksi elektris. Saat menempatkan hub pasif, Anda harus memerhatikan keterbatasan jarak.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

3.2 Layer Fisik di Jaringan Wireless

Jaringan wireless menggunakan gelombang radio (Radio Frequency/RF) atau gelombang mikro untuk melangsungkan komunikasi antarperangkat jaringan komputer. Jaringan wireless merupakan alternatif yang lebih modern untuk melakukan interkoneksi dibandingkan dengan jaringan kabel biasa yang menggunakan kabel tembaga maupun serat optik.

Jaringan wireless mempunyai keuntungan dan kerugian. Keuntungan yang paling utama adalah mobilitas serta terbebasnya perangkat jaringan dari belitan kabel. Kerugiannya adalah adanya interferensi radio oleh cuaca, peralatan wireless lain, atau bahkan halangan gedung seperti tembok, pepohonan, atau perbukitan.

Jaringan wireless menawarkan berbagai keuntungan dan semakin populer pada skala jaringan rumahan hingga jaringan berskala besar dalam sebuah perusahaan. Teknologi wireless merupakan teknologi yang banyak dikembangkan dan diperbaiki, sehingga ongkos produksi massalnya akan semakin rendah. Jaringan wireless yang sangat populer adalah jaringan Wireless Local Area Networking (WLAN) yang standarisasi oleh IEEE (Institute of Electrical and Electronic Engineers).

Jaringan wireless semakin berkembang dan mempunyai perkembangan teknologi yang semakin maju. Beberapa vendor pun telah menyediakan perangkat jaringan fisik yang semakin beragam dengan tujuan melakukan interkoneksi antar mode-node untuk dapat saling bertukar data maupun resource. Protokol yang dikenal di Wireless Local Area Network (WLAN) adalah IEEE 802.xx.

Apa arti dari 802.xx? Anda tentu bertanya-tanya mengapa standarisasi ini diberi nama kode dengan awalan angka 802. IEEE 802 merupakan subkomite yang bekerja untuk melakukan standarisasi jaringan baik jaringan lokal maupun jaringan metropolitan. Komite ini bertemu pada bulan Februari 1980, sehingga mereka memberikan nama proyek ini sebagai nama standar yang mereka bentuk. Angka '80' berasal dari angka tahun, sedangkan '2' berasal dari angka pada bulan kedua, yaitu bulan Februari. Ada beberapa standar kategori 802 yang terus berkembang, antara lain:

Standar	Topik
802.1	LAN/MAN Management dan Media Access Control Bridges
802.2	Logical Link Control
802.3	CSMA/CD
802.4	Token Bus
802.5	Token Ring
802.6	Distributed Queue Dual Bus (DQDB) Metropolitan Area Network (MAN)
802.7	Broadband Local Area Networks
802.8	Fiber-Optic LAN dan MAN
802.9	Integrated Services LAN Interface
802.10	LAN/MAN Security
802.11b	Wireless LAN
802.12	Demand Priority Access Method
802.15	Wireless PAN (Personal Area Network)
802.16	Broadband Wireless Access

3.2.1 Proyek 802

Pada subbab sebelumnya telah dijelaskan asal mula penamaan standar 802. Aturan penamaan dari setiap standar baru ialah dengan memberi angka di belakang angka 802 yang dipisahkan oleh tanda baca titik. Huruf yang letaknya di belakang angka 802 menunjukkan versi yang berbeda atau interpretasi lain yang berbeda dengan standar dasarnya.

3.2.1.1 802.1 LAN/MAN Management dan Media Access Control Bridges

IEEE 802.1 membicarakan standar pengaturan LAN serta MAN, dan juga MAC Bridge. Standar ini salah satunya menghasilkan algoritma spanning tree untuk bridge jaringan. Algoritma spanning tree digunakan untuk menghindari loop bridge pada jaringan multibridge.

3.2.1.2 802.2 Logical Link Control

Standar ini menentukan operasi sublayer Logical Link Control (LLC) dari layer Data Link pada model OSI. Sublayer LLC menyediakan interface antara sublayer MAC dan layer Network. Standar 802.2 digunakan pula pada spesifikasi Ethernets IEEE 802.3.

3.2.1.3 802.3 CSMA/CD

Standar ini digunakan pada jaringan dengan topologi bus, baseband signaling, dan metode akses jaringan CSMA/CD. Standar ini digunakan untuk menyesuaikan antara teknologi jaringan ethernet Digital, Intel, dan Xerox (DIX). Beberapa pengguna telah mengimplementasikan standar 802.3, yaitu dengan menggabungkannya dengan standar ethernet DIX atau sering disebut ethernet saja. Hasil implementasinya sudah digunakan pada seluruh standar 802 karena sederhana dan murah. Working group 802.3u merupakan versi update dari 802.3 yang menyertakan implementasi 100BaseT.

3.2.1.4 802.4 Token Bus

Standar ini menetapkan topologi bus secara fisik maupun logical dengan menggunakan kabel coaxial maupun serat optik serta metode akses media token passing. Standar ini digunakan secara umum untuk mengotomatisasi industri. Standar ini hampir sama dengan Manufacturing Automation Protocol (MAP), yang dikembangkan oleh General Motor dan telah digunakan pula pada industri-industri umum.

3.2.1.5 802.5 Token Ring

Token ring merupakan standar yang dikembangkan oleh IBM pada tahun 1984, baru setelah itu diikuti oleh standar 802.5. Standar 802.5 dan token ring merupakan standar yang sangat identik.

Seperti pada ethernet, token ring dapat menggunakan beberapa tipe kabel. Akan tetapi, kabel yang sering digunakan adalah kabel twisted-pair shielded maupun yang unshielded. Shielding ini berfungsi sebagai pelindung dari sinyal-sinyal elektris yang tidak diinginkan.

3.2.1.6 802.6 Distributed Queue Dual Bus (DQDB) Metropolitan Area Network

Seperti pada Wide Area Network, Metropolitan Area Network dapat mendukung secara simultan beberapa komputer. Standar teknologi ini direkomendasikan untuk digunakan pada MAN, yaitu standar Distributed Queue Dual Bus (DQDB).

3.2.1.7 802.7 Broadband Local Area Networks

Teknologi broadband digunakan pada TV kabel, di mana kabel tersebut akan membawa beberapa sinyal sekaligus. Metode pembagian sinyal pada beberapa frekuensi ini disebut Frequency Division Multiplexing (FDM).

3.2.1.8 802.8 Fiber-Optic LAN and MAN

Jaringan standar 802.8 adalah jaringan serat optik yang juga didefinisikan pada standar 802.3 hingga 802.6 dengan memasukkan standar Fiber Distributed Data Interface (FDDI) dan 10BaseFL. 10BaseFL adalah ethernet yang dapat dijalankan pada kabel serat optik.

3.2.1.9 802.9 Integrated Services (IS) LAN Interface

Standar ini didasarkan pada layanan Integrated Services Digital Network (ISDN), namun sudah jarang digunakan. Teknologi ISDN telah digantikan dengan teknologi kabel modem asymmetrical digital subscriber line (ADSL) dengan penggunaan lebih, performa tinggi, dan murah.

3.2.1.10 802.10 LAN/MAN Security

Standar ini menyediakan keamanan jalur data yang melewati jalur yang di-sharing. Penerapan standar ini digunakan pada Internet publik sebagai backbone untuk private interconnection antarlokasi. Bentuk dari penerapan standar ini disebut virtual private networking (VPN).

3.2.1.11 802.11 Wireless LAN

Wireless networking biasanya membutuhkan investasi yang lebih besar jika dibanding dengan jaringan cable-based. Kompensasi biaya ini telah tergantikan dengan kemampuan mobile pada setiap station yang ber-

gabung dalam jaringan perusahaan. Saat ini standar 802.11 telah di-update menjadi 802.11b, di mana standar ini mempunyai kecepatan lebih baik. Selain itu, standar teknologi tersebut terus diperbarui hingga saat ini.

3.2.1.12 802.12 Demand Priority Access Method

Standar ini mengombinasikan konsep ethernet dengan ATM (Asynchronous Transfer Mode). Skema komunikasi ini disebut Demand Priority, yang menggunakan hub yang lebih cerdas dalam mengalokasikan bandwidth yang lebih besar. Hub akan melakukan scan pada port-port, kemudian mengalokasikan bandwidth berdasarkan prioritas frame. Fitur ini sangat bermanfaat pada transmisi super besar, seperti real-time audio dan video.

Standar 802.12 juga disebut 100 VG (Voice Grade), 100 VGAnyLAN, 100 BaseVG, dan AnyLAN. Angka 100 merupakan kependekan dari 100 Mbps, di mana kecepatan ini 10 kali lebih besar dibandingkan dengan ethernet.

Beberapa fitur utama teknologi jaringan adalah:

Teknologi	Kecepatan	Metode Akses	Topologi	Media
IEEE 802.3	10, 100, 1000 Mbps	CSMA/CD	Bus logical	Coaxial atau UTP
IEEE 802.5	4 atau 16 Mbps	Token Passing	Star fisikal, ring logical	STP
IEEE 802.11b	1 atau 11 Mbps	CSMA/CA	Celullar	Wireless
FDDI	200 Mbps	Token Passing	Star fisikal, ring logical	Serat Optik

3.2.2 IEEE 802.11

Di pasaran terdapat bermacam-macam merek, model, dan cara pembuatan peralatan RF. Heterogenitas dan banyaknya merek, model, dan jenis peralatan menjadikan user sangat kesulitan untuk menentukan standarisasi peralatannya. Seiring dengan perkembangan yang semakin pesat, beberapa pabrikan jaringan RF wireless mempunyai metode berbeda dalam mengembangkan frekuensi, skema encoding, jenis antena, dan protokol jaringan wireless. Banyaknya variasi jenis tentu saja tidak menguntungkan pengguna. Untuk itu, pada jaringan wireless ditetapkan standarisasi peralatan wireless yang disebut standarisasi IEEE 802.11.

IEEE 802.11 merupakan standar untuk produk-produk WLAN yang telah dikenal pengguna jaringan pada umumnya. IEEE merupakan sebuah organisasi independen yang mengatur beberapa standar dalam jaringan lokal dengan menggunakan media kabel dan jaringan wireless. Komite standarisasi IEEE 802 membentuk standar jaringan WLAN pada tahun 1990, di mana standarisasi ini telah dikembangkan menjadi standar global peralatan radio dan jaringan yang beroperasi pada frekuensi 2.4 GHz. Perkumpulan ini telah mengembangkan standar pada frekuensi bebas dengan data rate 1 dan 2 Mbps. Standar ini tidak mengacu pada teknologi atau implementasi tertentu, akan tetapi hanya standarisasi sederhana pada jaringan layer fisikal dan layer Media Access Control (MAC). Standarisasi ini mengizinkan pabrikan dari wireless LAN untuk mengembangkan peralatan jaringan dengan lebih leluasa.

Standar WLAN diawali dengan standar 802.11 yang diperkenalkan pada tahun 1997 oleh IEEE. Standar dasar ini dapat dipergunakan untuk melakukan transmisi data hingga 2Mbps. Dengan berkembangnya waktu, implementasi dari standar ini semakin populer dan meluas. Penambahan ekstensi di belakang 802.11 dipergunakan untuk mengenali beberapa perbaikan dan tambahan fitur dari standar yang telah ditentukan 802.11.

Standar 802.11b telah diratifikasi oleh IEEE pada bulan Juli 1999 dan beroperasi pada frekuensi radio ber-bandwith 2,4 GHz hingga 2,497 GHz. Metode modulasi yang dipilih untuk standar 802.11b disebut *Direct Sequence Spread Spectrum* (DSSS) dengan menggunakan *Complementary Code Keying* (CCK), sehingga kecepatan transmisi datanya mencapai 11 Mbps.

Pada tahun 1997, IEEE juga meratifikasi standar dari 802.11a, akan tetapi beberapa produk tidak menggunakan standar ini hingga tahun 2001. Standar ini tidak begitu dikembangkan seperti pada standar 802.11b. Standar ini beroperasi pada frekuensi radio 5,15 GHz dan 5,875 GHz. Standar ini menggunakan skema modulasi yang disebut *Orthogonal Frequency Division Multiplexing* (OFDM) dengan kecepatan transmisi data mencapai 54 Mbps.

Spesifikasi 802.11g diratifikasi pada bulan Juni 2003, di mana spesifikasi ini beroperasi pada frekuensi 2,4 GHz hingga 2,497 GHz (sama seperti pada spesifikasi 802.11b). Teknik modulasinya sama seperti pada

spesifikasi 802.11a, yaitu menggunakan teknik OFDM, sehingga dapat menghasilkan throughput (persentase perbandingan input dan outputnya) hingga 54 Mbps (sama seperti pada 802.11a). Kombinasi dari fitur ini menghasilkan infrastruktur yang lebih cepat, lebih murah, serta koneksi yang lebih luas. Pengguna 802.11b perlu melakukan upgrading agar kompatibel dengan produk 802.11g.

Tabel di bawah merupakan detail perkembangan standar 802.11.

802.11	Standar dasar WLAN yang mendukung transmisi data 1 Mbps hingga 2 Mbps
802.11a	Standar High Speed WLAN untuk 5 GHz band yang mendukung hingga 54 Mbps.
802.11b	Standar WLAN untuk 2,4 GHz band yang mendukung hingga 11 Mbps atau disebut Wi-Fi.
802.11e	Perbaikan dari QoS (Quality of Service) pada semua interface radio IEEE WLAN.
802.11f	Mendefinisikan komunikasi inter-access point untuk memfasilitasi beberapa vendor yang mendistribusikan WLAN.
802.11g	Menetapkan teknik modulasi tambahan untuk 2,4 GHz band, yang dimaksudkan untuk menyediakan kecepatan hingga 54 Mbps.
802.11h	Mendefinisikan pengaturan spektrum 5 GHz band yang digunakan di Eropa dan Asia Pasifik.
802.11i	Menyediakan keamanan yang lebih baik. Penentuan alamat di mana terdapat kelemahan keamanan pada protokol autentikasi dan enkripsi. --
802.11j	Penambahan pengalaman pada channel 4.9 GHz hingga 5 GHz untuk standar 802.11a di Jepang.

Untuk penjelasan selengkapnya, subbab berikut akan membahas secara mendetail perkembangan standar 802.11, 802.11a, 802.11b, dan 802.11g.

3.2.2.1 Standar Awal 802.11

Standar ini merupakan standar awal yang diratifikasi pada tahun 1977. Standar ini merupakan layer fisik yang menggunakan frequency hopping spread spectrum (FHSS) dan direct sequence spread spectrum (DSSS) yang beroperasi pada pita 2.4 GHz dengan data rate hingga 2 Mbps. FHSS menggunakan transmisi sinyal pita lebar yang menjangkau keseluruhan range 2.4 GHz, sehingga sangat dimungkinkan untuk melakukan tune access point FHSS menjadi 15 pola hopping yang berlainan serta tidak menimbulkan interferensi satu dengan yang lain. Hal ini akan menjadikan 15 FHSS access point tersebut dapat beroperasi dengan efektif pada area yang sama. Karena versi ini hanya mempunyai

data rate maksimum 2 Mbps, versi ini tidak banyak digunakan pada LAN wireless indoor. FHSS digunakan untuk menangani masalah jaringan wireless outdoor, point to point system, karena FHSS lebih tahan terhadap interferensi yang biasa terjadi pada lingkungan outdoor.

3.2.2.2 802.11a

Pada akhir 1999, IEEE mengeluarkan 802.11a yang beroperasi pada pita 5 GHz dengan menggunakan orthogonal frequency division multiplexing (OFDM) serta data rate hingga 54 Mbps. Namun, sampai tahun 2000 produk ini tidak tersedia karena terdapat kesulitan dalam hal pengembangan pada band 5 GHz. Standar ini secara aktual mempunyai jangkauan 50 m tergantung data rate-nya. Access point dan NIC dengan standar 802.11a mulai tersedia pada akhir tahun 2001.

Keuntungan utama dari standar 802.11a adalah kapasitasnya yang cukup tinggi, yaitu mencapai 12 channel yang terpisah secara non-overlapping, yang menjadikan standar ini sebagai pilihan yang tepat untuk mendukung aplikasi yang membutuhkan performa tinggi, seperti streaming video. Keuntungan lain adalah pita 5 GHz tidak begitu padat, sehingga user dapat menerima performa yang sangat tinggi. Perlu Anda ketahui bahwa beberapa peralatan seperti oven microwave dan telepon cordless menggunakan pita 2.4 GHz. Dengan potensi interferensi RF yang kecil, pengembangan sistem standar wireless ini tidak begitu berisiko.

Kekurangan dari standar ini adalah terbatasnya cakupan range pancamya karena menggunakan pita frekuensi 5 GHz, sehingga range cakupannya tidak lebih dari 50 m pada berbagai fasilitas. Akibatnya, standar ini memerlukan access point lebih banyak.

Standar 802.11a tidak kompatibel dengan 802.11b/g, sehingga kartu radio standar 802.11b tidak dapat bergabung dengan access point 802.11a, akan tetapi dapat beroperasi apabila dibalik. Beberapa vendor memecahkan masalah ini dengan cara memproduksi kartu radio yang dapat diimplementasikan pada standar 802.11a dan 802.11b.

3.2.2.3 802.11b

Bersama standar 802.11a, IEEE juga meratifikasi standar baru 802.11b, yaitu dengan menambahkan rate yang lebih tinggi dibanding dengan

standar asli direct sequence pada pita 2.4 GHz hingga data rate 11 Mbps. Access point dan NIC radio standar ini telah tersedia di pasaran sejak tahun 1999. Saat ini, standar ini menjadi standar yang paling banyak digunakan.

Keuntungan yang sangat signifikan dari keberadaan standar 802.11b adalah mempunyai range yang relatif panjang hingga 100 m pada fasilitas dalam gedung. Range ini sangat efektif dipergunakan untuk mengembangkan LAN secara wireless dibandingkan dengan standar sebelumnya.

Kerugian saat menggunakan standar 802.11b adalah penggunaan channel pada pita 2.4 GHz dibatasi, yaitu hanya 3 buah channel, sedangkan standar 802.11 menggunakan 14 channel untuk melakukan konfigurasi access point. Beberapa perusahaan hanya menggunakan channel 1, 6, dan 11 untuk pemasangan access point, namun antara satu dengan yang lain tidak timbul interferensi. Pembatasan secara keseluruhan kapasitas 802.11b membuat dukungannya pada performa aplikasi menengah, seperti aplikasi e-mail atau web surfing, menjadi lebih baik.

Kerugian lain adalah terdapatnya kemungkinan interferensi RF dengan peralatan radio yang lain, seperti telepon cordless dan oven microwave 2.4 GHz karena akan mengurangi secara signifikan performa dari standar ini. 802.11b menggunakan DS-SS untuk menyebarkan sinyal frame data melalui 22 MHz, yang merupakan bagian dari pita frekuensi 2.4 GHz, sehingga menjadi kebal terhadap interferensi RF.

3.2.2.4 802.11g

IEEE meratifikasi standar 802.11 pada tahun 2003. Standar ini kompatibel dengan 802.11b dan dapat meningkatkan performa hingga 54 Mbps pada pita frekuensi 2.4 GHz dengan menggunakan OFDM.

Keunggulan dari standar 802.11g adalah kompatibilitasnya dengan standar sebelumnya, yaitu 802.11b. Beberapa perusahaan yang telah menggunakan jaringan 802.11b meng-upgrade access point mereka ke standar 802.11g dengan cara cukup sederhana. Selanjutnya, migrasi ini menjadikan pengembangan wireless LAN sangat efektif. Yang menjadi pertanyaan adalah apakah ada beberapa keterbatasan saat klien menggunakan peralatan jaringan 802.11b pada lingkungan standar 802.11g?

Permasalahannya ialah karena peralatan dengan standar 802.11b tidak memahami transmisi peralatan 802.11g. Hal ini dikarenakan perbedaan modulasi pada kedua tipe ini.

Kerugian yang lain adalah adanya interferensi RF secara potensial dan keterbatasan dari tiga channel yang tidak saling overlap pada standar 802.11g karena standar ini masih menggunakan frekuensi 2.4 GHz yang sarat dengan interferensi.

3.2.3 Channel

Pemahaman tentang channel sangat penting sebab hal ini berkaitan dengan kapasitas secara keseluruhan dari WLAN. Channel merupakan sebuah bagian pada pita atau band frekuensi radio. Ada sejumlah kecil bandwidth yang membawa data saat modulasi frekuensi radio berada di band sebuah frekuensi. Bagian ini sangat penting agar setiap frekuensi tidak saling bertumpuk (overlap), sehingga jaringan akan tersusun dalam urutan data paket tertentu saat dikirimkan.

Spesifikasi 802.11a beroperasi pada frekuensi radio antara 5,15 GHz dan 5,875 GHz, sedangkan spesifikasi 802.11b dan 802.11g beroperasi pada range frekuensi radio 2,4 GHz hingga 2,497 GHz. Anda dapat melihat bahwa 802.11a mempunyai pita atau band frekuensi yang lebih luas yang dapat menampung lebih banyak channel pada keseluruhan throughputnya. Frekuensi yang luas ini menjadikan 802.11a mendukung hingga 8 non-overlapping channel, sedangkan 802.11b/g hanya mendukung 3 non-overlapping channel. Perlu Anda ketahui bahwa setiap negara mempunyai kebijaksanaan range frekuensi serta channel yang berlainan.

Setiap channel akan membawa throughput secara maksimum dari standar yang ditentukan. Oleh karena itu, standar 802.11b dan 802.11g mempunyai 3 non-overlapping channel yang akan membawa 11 Mbps throughput (total 33 Mbps) dan 54 Mbps throughput (162 Mbps). Sementara itu, standar 802.11a mempunyai standar maksimum 8 non-overlapping channel yang akan membawa 54 Mbps setiap throughput-nya, atau total throughput-nya adalah 432 Mbps.

Keuntungan dari 802.11b adalah teknologi standar ini telah sangat luas dikembangkan dan mempunyai penetrasi yang sangat baik pada dinding-dinding bangunan dengan range indoor, sehingga sangat cocok untuk



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

pada standar 802.11. Wi-Fi Alliance pertama kali membentuk Wireless Ethernet Compatibility Alliance (WECA), sebuah organisasi nonprofit yang mempunyai fokus pada pemasaran serta mengurusi interoperabilitas pada produk wireless LAN 802.11. Wi-Fi Alliance juga memprakarsai standar keamanan pada 802.11i yang disebut Wi-Fi Protected Access (WPA).

Sertifikasi Wi-Fi adalah proses untuk memastikan interoperabilitas antar-peralatan wireless LAN 802.11, termasuk access point dan kartu-kartu jaringan radio wireless yang biasanya mempunyai beberapa form factor yang sangat beragam. Perusahaan-perusahaan produsen peralatan wireless harus menjadi anggota Wi-Fi Alliance. Perusahaan-perusahaan tersebut memerlukan sertifikasi Wi-Fi untuk menjaga kualitas produk. Sertifikasi ini juga digunakan untuk menjaga interoperabilitas beberapa produk Wi-Fi. Setelah produk tersebut melalui beberapa tes, pabrikan akan diberikan hak untuk menempatkan logo sertifikasi Wi-Fi, sehingga user mudah mengenalinya. Setelah produk melalui tes standarisasi yang teruji, user akan mendapatkan beberapa kemudahan dalam hal standarisasi dan interoperabilitas.

3.2.6 Ad Hoc

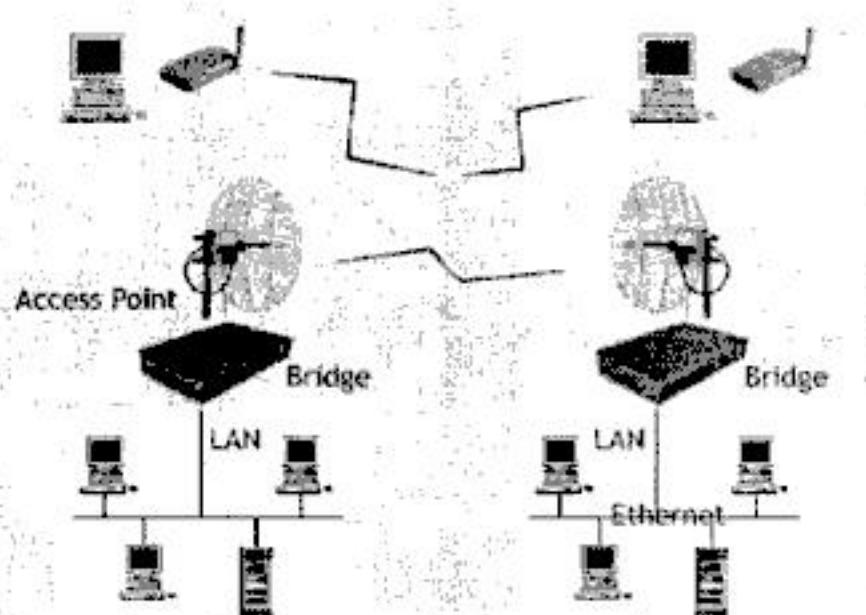
Standarisasi IEEE 802.11 mendefinisikan protokol dalam dua tipe jaringan, yaitu jaringan Ad Hoc dan Client/Server.

Jaringan **Ad Hoc** merupakan jaringan sederhana di mana komunikasi terjadi di antara dua perangkat atau lebih pada cakupan area tertentu tanpa harus memerlukan sebuah access point atau server. Standarisasi ini semacam etiket pada setiap perangkat jaringan dalam melakukan akses media wireless. Metode ini meliputi penentuan pemberian permintaan koneksi pada sebuah media untuk memastikan *throughput* yang dimaksimalkan untuk pengguna dalam menerima layanan.

Komunikasi Ad Hoc menggunakan media gelombang radio satu dengan yang lain, dan peralatan ini akan mengenal peralatan RF lain dalam cakupan sinyal yang saling berdekatan, sehingga komunikasi dapat dilakukan. Jaringan Ad Hoc dapat digunakan pada komputer-komputer notebook, laptop, atau peralatan handheld lain yang membutuhkan



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 3-4 Jaringan Multipoint RF

3.2.8 Pengembangan Konfigurasi Wireless

Konfigurasi jaringan wireless yang lain telah berkembang seiring dengan berkembangnya kebutuhan pengembang maupun implementator lain. WLAN telah dikonfigurasikan dengan beberapa cara serta dengan range yang berlainan tergantung dari kebutuhan pengembangan jaringan access point dengan coverage yang luas hingga hanya beberapa puluh meter yang sering disebut *hotspot*.

3.2.8.1 Infrastruktur Jaringan

Infrastruktur jaringan tersusun dari klien WLAN yang terkoneksi pada jaringan corporate melalui access point wireless dan beroperasi seperti pada jaringan LAN kabel biasa. Beberapa jaringan corporate yang dibangun secara wireless dapat digabungkan dengan akses ke jaringan kabel biasa untuk melakukan koneksi ke file server dan printer.

3.2.8.2 Hotspot

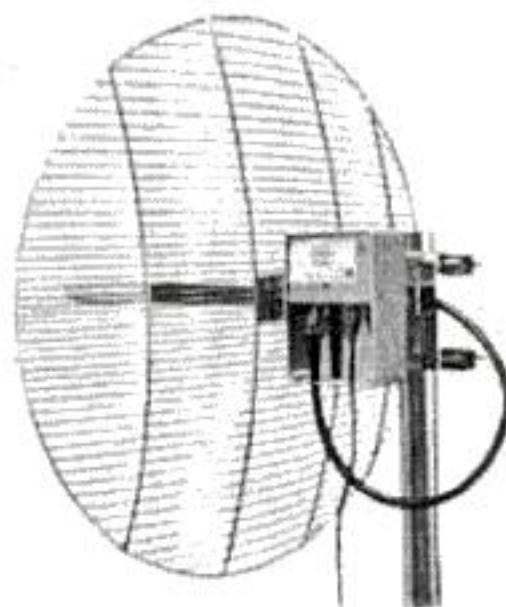
Hotspot menyediakan layanan wireless LAN baik gratis maupun dengan pungutan biaya. Beberapa sudut area umum telah dijadikan area hotspot untuk dapat melakukan akses ke layanan access point. Dengan menggunakan area hotspot, beberapa notebook yang telah disertifikasi untuk dapat melakukan koneksi teknologi WLAN dapat dengan mudah menggunakan resource jaringan tersebut. Notebook ini dapat melakukan pengiriman dan penerimaan data di manapun selama masih dalam coverage base station wireless LAN tersebut.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 3-7 Antena

Hal lain yang perlu diperhatikan dalam mengembangkan dan meng-aplikasikan WLAN selain hardware di atas adalah:

Interoperabilitas. Perhatikan selalu interoperabilitas antara infrastruktur sisi klien pada komponen-komponen WLAN. Produk-produk WLAN biasanya menyertakan sertifikasi yang dicantumkan pada setiap produk WLAN, sehingga jaminan interoperabilitas antarproduk WLAN dapat dipertanggungjawabkan.

Frekuensi. Pastikan untuk mengimplementasikan peralatan pada frekuensi yang tepat, seperti pemilihan channel yang tepat di access point. Contoh, produk 802.11a tidak dapat digunakan untuk berkomunikasi dengan 802.11b dan 802.11g karena keduanya memiliki frekuensi yang sama. Kedua produk tersebut mempunyai modulasi yang berbeda meskipun beroperasi pada frekuensi yang sama, sehingga membutuhkan desain mode operasi ganda atau upgrade untuk memastikan kompatibilitasnya.

Coverage. Penempatan access point pada area yang strategis akan menyediakan cakupan coverage yang maksimal. Hal yang harus dihindari adalah menempatkan access point berhadapan atau berdekatan dengan tembok pada area tertentu. Perhitungan coverage area yang memerhatikan kesinambungan koneksi (seperti pada roaming di sistem selular) sangat penting, selain itu juga harus memperhitungkan overlapping coverage. Pengaturan band frekuensi digunakan untuk menghindari tabrakan sinyal yang dapat menurunkan performa saat paket data diurutkan.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

butuhkan alat tambahan sebagai alternatifnya, seperti penambahan antena yang directive.

Beberapa access point telah menyediakan NIC untuk kartu PC radio yang dapat dengan mudah diganti-ganti untuk mengakomodasi munculnya teknologi baru seperti 802.11a atau 802.11g. Pada beberapa kasus, pengguna dapat melakukan upgrade radio NIC dengan cukup mudah, sehingga akan memperpanjang usia pakai access point tersebut.

3.3.1.4 Mini PCI

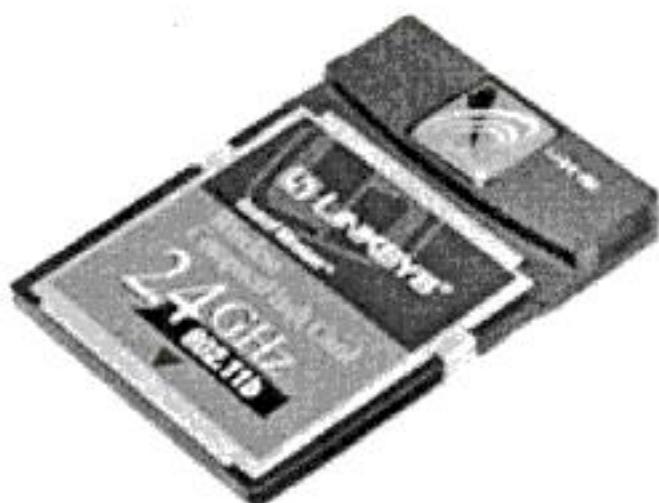
Mini PCI merupakan versi kecil dari kartu PCI standar. Mini PCI memiliki fitur dan fungsi yang sama dengan kartu PCI standar normal, hanya saja ukurannya seperempat kali lebih kecil. Kartu mini PCI dapat diintegrasikan pada laptop, dan antena yang ditempatkan di sisi luar terintegrasi pada monitor atau LCD Screen.

Mini PCI hampir tidak memiliki kelemahan jika dibandingkan dengan PCI standar, hanya saja prosedur pemasangannya lebih sulit karena harus membongkar laptop. Laptop yang telah digaransi oleh pabrikan tentu saja tidak dapat dengan leluasa dibongkar, karena garansi yang dijanjikan tentunya akan hilang setelah Anda membongkar fisik laptop Anda.

3.3.1.5 Compact Flash

Compact Flash (CF) diperkenalkan pada tahun 1994 oleh SanDisk Corporation. CF mempunyai bentuk yang sangat kecil, tipis, dan dengan berat yang sangat ringan jika dibandingkan dengan kartu PC. CF juga mempunyai kebutuhan catu daya yang sangat kecil, sehingga tidak begitu boros baterai dibanding dengan kartu PC. CF biasanya digunakan pada PDA karena bentuknya yang begitu kecil dan compact.

Beberapa peralatan wireless ini berkembang dengan pesat. Saat buku ini ditulis, beberapa produk telah muncul untuk memperkaya dan mengoptimalkan produk-produk yang telah ada. Beberapa peralatan seperti Secure Digital telah muncul dengan bentuk fisik yang semakin mengecil. Beberapa pabrikan juga telah memproduksi adapter-adapter eksternal yang dapat dikoneksikan via port USB dengan cukup mudah.



Gambar 3-10 Contoh Compact Flash

3.3.2 Keamanan Jaringan Wireless

Masalah keamanan jaringan selalu menjadi prioritas penting dalam pengembangan jaringan baik wired maupun wireless. WLAN mempunyai kemampuan fleksibilitas pengembangan yang sangat tinggi. Akan tetapi, fitur ini justru menimbulkan beberapa keterbukaan yang potensial terhadap adanya akses-akses yang tidak diinginkan. Akses ilegal terhadap jaringan wireless access point Anda akan mudah dilakukan apabila Anda tidak mempersiapkan proteksi data yang lebih baik. Untuk itu, beberapa teknologi keamanan jaringan telah dikembangkan dengan berbagai tingkatan proteksi untuk keperluan jaringan wireless dari home user hingga bisnis skala besar.

Saat ini, spesifikasi produk 802.11b telah dilengkapi dengan keamanan standar dengan jenis proteksi:

3.3.2.1 Service Set Identifier (SSID)

Merupakan kunci identitas WLAN yang telah umum digunakan. Klien harus dikonfigurasikan dengan menggunakan SSID yang benar untuk dapat melakukan akses ke jaringan WLAN. Kunci ini harus dapat di-share hanya pada mereka yang telah sah untuk melakukan akses jaringan. SSID harus dapat diubah-ubah secara periodik untuk lebih meningkatkan keamanan.

3.3.2.2 Media Access Control (MAC)

Filtering pada alamat-alamat tertentu untuk membatasi akses WLAN ke daftar komputer yang dapat dibuat pada setiap access point.

3.3.2.3 Wired Equivalent Privacy (WEP)

Skema enkripsi yang melindungi aliran data WLAN antara klien dan access point yang telah ditentukan oleh standar 802.11. Fitur ini harus diaktifkan walaupun fitur ini terkadang mengalami kerusakan atau ketidakefisienan keamanan.

Selain fitur keamanan standar, para vendor jaringan pun telah mengembangkan beberapa mekanisme proteksi secara proprietary. Industri hardware serta industri jaringan telah berkolaborasi untuk membentuk sistem infrastruktur untuk dapat melakukan proteksi, interoperable, serta kemudahan dalam mengatur ekosistem mobile wireless. Beberapa fitur keamanan yang lain akan dibahas pada bab selanjutnya.

3.3.3 Pencegahan Keamanan Jaringan yang Lain

Dari beberapa model pengamanan jaringan yang telah dibahas di bagian terdahulu, masih ada beberapa hal yang menyangkut pengembangan maupun pengaturan-pengaturan yang harus selalu diperhatikan. Masalah keamanan jaringan ini dapat menjadi permasalahan laten yang tidak akan berhenti berkembang, sehingga updating serta pengembangan teknologi akan selalu terjadi ke arah yang lebih baik. Beberapa permasalahan jaringan wireless yang lain adalah:

3.3.3.1 Pemasangan Access Point Sembarangan

Anda harus melakukan auditing atau pemeriksaan reguler terhadap beberapa access point yang telah dipasang untuk menanggulangi serta mengidentifikasi celah-celah keamanan yang diakibatkan oleh konfigurasi access point sembarangan. Pemasangan access point yang sembarangan dapat terjadi karena memang disengaja dan tanpa sepengetahuan pihak administrator pengelola jaringan atau bagian yang memang bertanggung jawab terhadap masalah jaringan. Pemasang memang sengaja tidak mengonfigurasi saat memasang access point, sehingga membuka kesempatan terjadinya akses-akses ilegal pada jaringan.

3.3.3.2 Virtual Private Network (VPN)

Teknologi ini menawarkan keamanan tambahan dengan membuat sistem *tunel* yang akan membungkus data dari akses-akses umum jaringan di

Internet dengan menggunakan proses enkripsi dan dekripsi pada proses transmisi data. Penerapan keamanan jaringan ini telah semakin umum digunakan pada klien VPN untuk melakukan akses jaringan intern perusahaan menggunakan beberapa access point wireless.

3.4 Antena

Pembahasan mengenai media fisik wireless ini belum lengkap jika belum membahas antena secara mendetail. Antena merupakan media yang sangat vital dalam memaksimalkan coverage radio frekuensi. Luasnya area cakupan sebuah jaringan wireless merupakan perhatian utama semua pengembang jaringan wireless LAN. Jika Anda mengabaikan permasalahan antena, maka range efektif sebuah access point tidak akan mencapai tingkat maksimal dalam hal coverage areanya. Permasalahan ini akan mengakibatkan kesalahan dalam hal perencanaan pengembangannya, sehingga akhirnya akan menyebabkan terjadinya kekeliruan dalam menentukan biaya pengembangan. Solusinya adalah melakukan penentuan konfigurasi yang sesuai dengan area cakupan yang optimal, sehingga jumlah access point akan optimal.

3.4.1 Dasar Antena

Antena merupakan pasangan dari energi gelombang Radio Frequency (RF) yang merambat melalui media udara. Energi elektronis akan bergerak dari satu tempat ke tempat lain dalam satu jalan, yaitu energi mengalir melalui konduktor, kemudian melalui udara dalam bentuk gelombang tidak terlihat. Pada sistem wireless, energi elektronis akan mulai mengalir pada konduktor, kemudian berubah menjadi gelombang yang merambat melalui udara, lalu mengalir ke konduktor kembali.



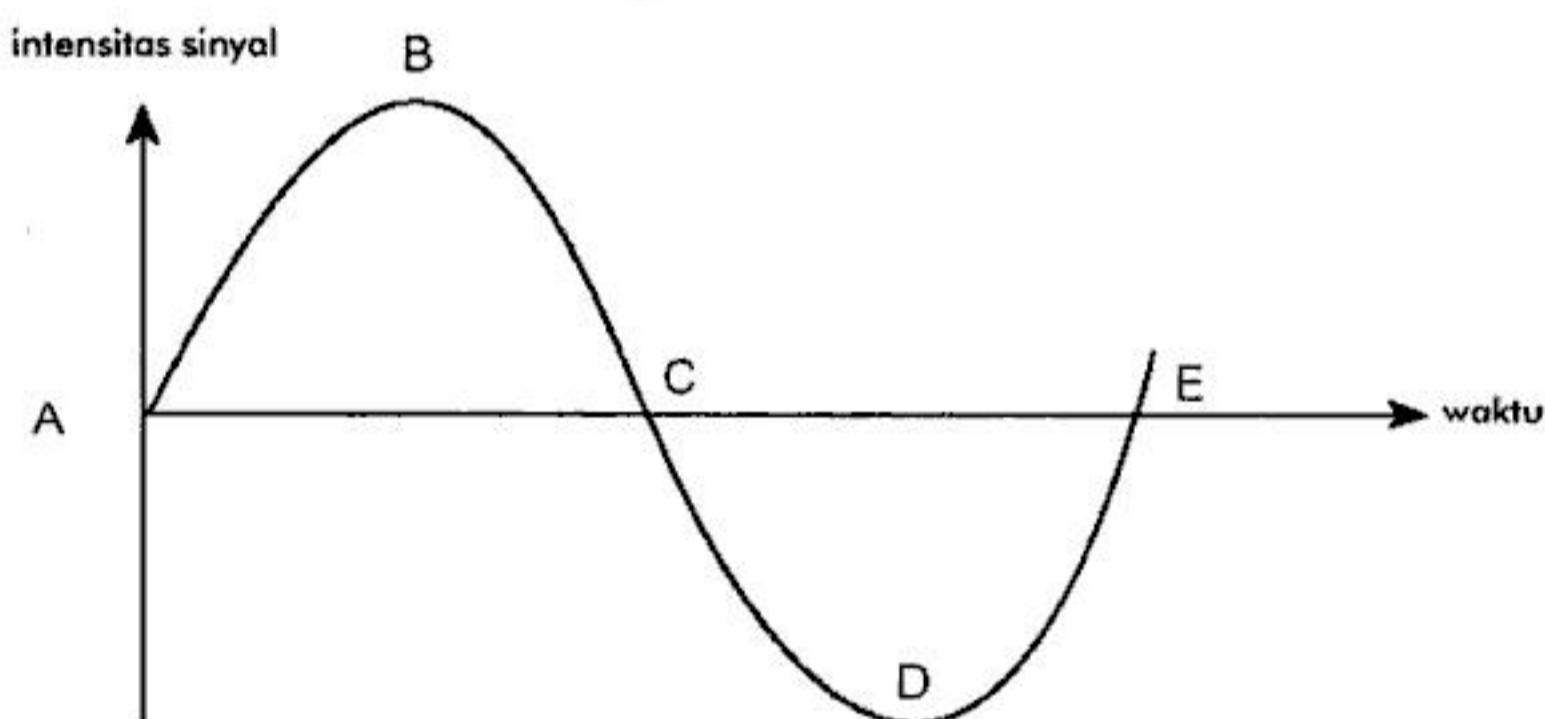
Gambar 3-11 Konsep Dasar Wireless

Pada Gambar 3-11, sinyal elektrik akan merambat di konduktor pada kotak yang diberi tanda 'T'. Kotak T berarti transmitter (pemancar) yang akan mengubah arus sinyal elektrik ke gelombang udara. Setelah melalui perjalanan dengan kecepatan tinggi, sinyal tersebut akan mencapai kotak yang diberi tanda 'R' yang berarti receiver (penerima) yang akan mengubah gelombang udara menjadi tegangan elektrik.

Transmitter yang ada di NIC radio atau di access point akan mengirimkan sebuah sinyal RF ke antena, yang akan bertindak sebagai radiator serta akan mengalirkan sinyal ke udara. Antena juga beroperasi dengan proses bolak-balik dengan menangkap sinyal RF dari udara, selanjutnya akan diterima oleh receiver.

3.4.1.1 Sinyal Analog

Energi elektrik (arus atau gelombang) dapat menyimpan informasi jika dibuat dalam variasi tertentu dan satuan waktu tertentu pula (disebut intensitas). Variasi energi elektrik tersebut diberi istilah sinyal (signal). Sinyal dibagi menjadi dua jenis, yaitu analog dan digital. Gelombang sinus adalah contoh sebuah sinyal analog. Gelombang ini dapat mengalir melalui kabel ataupun udara. Anda dapat melihat variasi gelombang sinyal sinus (intensitas) pada Gambar 3-12.



Gambar 3-12 Gambar Gelombang Sinus

Di dunia Radio Frequency (RF), intensitas dari sinyal dapat diukur kekuatannya. Waktu yang dibutuhkan sinyal hingga menyelesaikan



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



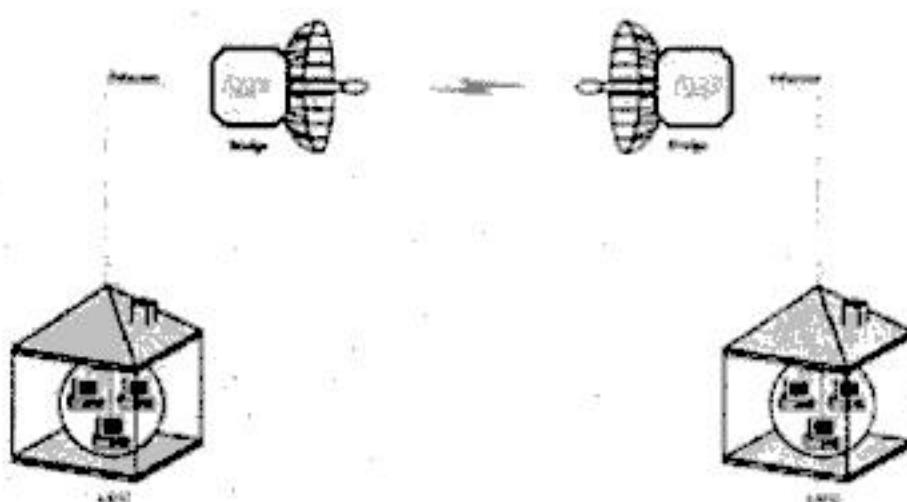
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 3-18 Menghubungkan Antargedung

3.4.4 Metode Penyebaran Spektrum

Spesifikasi IEEE 802.11 mencakup beberapa metode transmisi data. Metode pertama merupakan definisi standar metode jaringan wireless tanpa lisensi. Metode kedua mempunyai cara transmisi data yang sama, yaitu menggunakan gelombang radio, seperti teknologi bluetooth pada gadget dan perangkat mobile yang lain, sedangkan metode ketiga menggunakan sinar inframerah.

Metode inframerah mempunyai perkembangan teknologi yang masih terbatas, di mana teknologi ini hanya dapat mentransmisikan data pada jarak yang sangat pendek. Teknologi yang berkembang sangat pesat adalah teknologi gelombang radio atau radio frequency (RF), yaitu Direct Sequence Spread Spectrum (DSSS) dan Frequency Hopping Spread Spectrum (FHSS). Anda harus memahami kedua teknologi tersebut serta performanya karena sangat penting untuk memahami teknologi mana yang efektif digunakan, sehingga Anda dapat membandingkan keduanya dan pada akhirnya akan membantu Anda dalam mengembangkan jaringan wireless secara lebih tepat guna.

3.4.4.1 Direct Sequence

Metode Direct Sequence Spread Spectrum (DSSS) menggunakan carrier yang fix pada pita frekuensi tertentu. Sinyal data ditransmisikan menggunakan pita narrowband serta menggunakan komunikasi gelombang mikro. Skema encoding pada metode ini disebut pseudonoise sequence, atau PN sequence.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

lebih rendah pada keseluruhan transmisi. Secara keseluruhan, DS menggunakan bandwidth lebih tinggi bila dibandingkan dengan sistem FH.

Direct Sequence	Frequency Hopping
Waktu latency pendek	Waktu latency panjang
Processing gain konstan=rasio signal to noise yang lebih baik	Tanpa processing gain
Lock-in dengan cepat karena menggunakan sinkronisasi Radio	Lock-in dengan lambat karena harus melakukan pencarian channel
Tidak menggunakan dwell time	400 mikro detik dwell time
Range indoor yang pendek	Range indoor yang pendek
Range outdoor yang panjang hingga 40 Km	Range outdoor pendek hingga 10 Km
Troughput data secara keseluruhan lebih besar	Troughput data secara keseluruhan kecil

3.5 Pengaturan Akses dengan Access Point

Pengaturan akses sebuah komponen digunakan untuk keperluan keamanan, menjaga kualitas layanan (Quality of Service/QoS), dan mekanisme roaming dalam jaringan wireless standar. Proses ini digunakan untuk memperkuat sistem keamanan wireless secara keseluruhan. Komponen yang menjadi tumpuan dalam hal ini adalah hardware yang digunakan sebagai pengatur akses, baik dari jaringan kabel maupun wireless, yaitu access point.

Pengatur akses ini akan digunakan untuk menyediakan pemusatan dan regulasi lalu lintas antara jaringan wireless yang terbuka dengan resource yang berada di belakang komponen. Sebagai contoh, apabila jaringan LAN akan berhubungan dengan Internet, maka pengatur akses akan melakukan autentikasi dan memberi hak pengguna mana yang dapat menggunakan resource internal serta mengatur regulasi akses. Beberapa keuntungan dengan adanya access point adalah:

Biaya yang rendah – Access point dengan fungsi khususnya secara keseluruhan menghasilkan biaya sistem lebih rendah. Dalam membangun jaringan wireless yang luas dibutuhkan jumlah access point yang optimal untuk menghasilkan coverage dan performa yang luas. Dengan jumlah



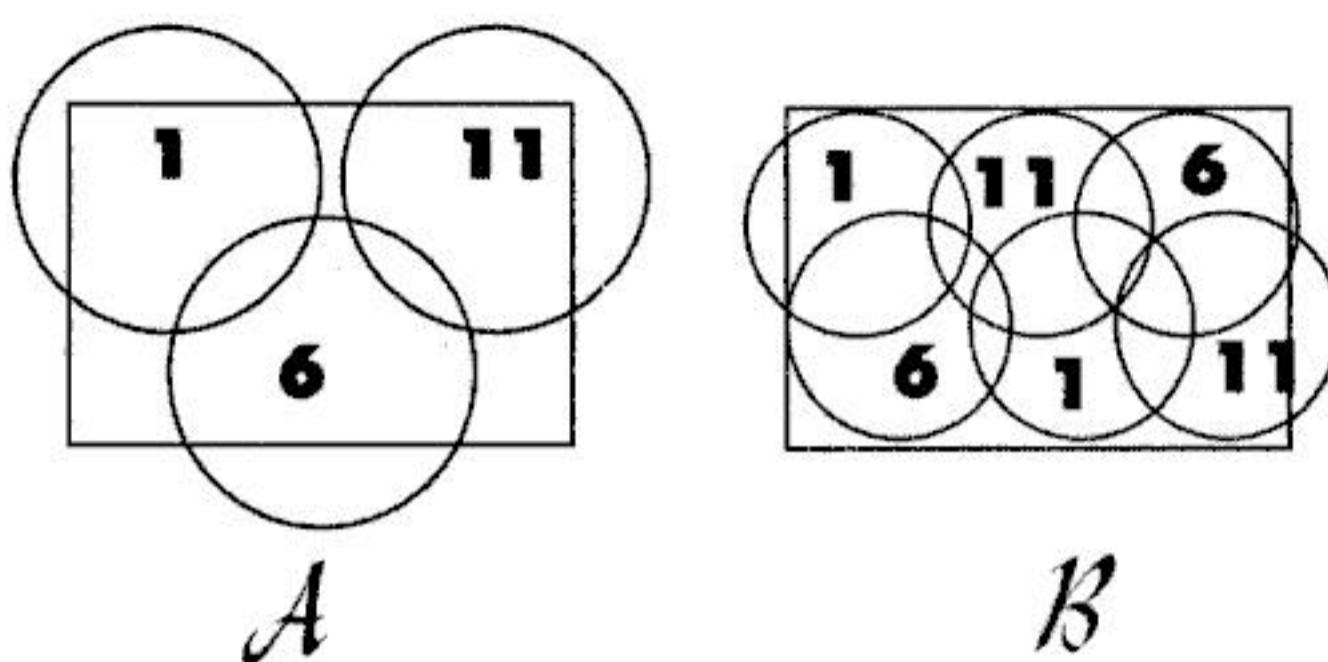
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 3-22 Model Layout Penempatan Access Point

Pada penempatan model layout A, sel coverage access point terlalu luas walaupun jumlah access point lebih sedikit dengan power transmit besar. Pada layout penempatan model B, dengan mengurangi power access point menjadikan coverage menjadi lebih kecil, namun jumlah access point menjadi lebih banyak.

Service set identifier (SSID). SSID merupakan nama WLAN yang telah diasosiasikan oleh pengguna. Secara default, SSID diatur dengan nilai yang umum digunakan. Untuk meningkatkan keamanan jaringan, Anda harus melakukan perubahan SSID dengan nilai yang berlainan dengan defaultnya, maksudnya untuk menghindari user yang tidak berhak mengakses access point. Untuk meningkatkan keamanan, beberapa access point dapat mematikan fungsi broadcast SSID. Hal ini digunakan untuk menghindari beberapa klien yang menggunakan sistem operasi tertentu (Contoh: Windows XP) dari akses yang tidak berhak.

Data Rate. Beberapa access point telah mengidentifikasi data rate mana yang dapat dipergunakan. Secara default, access point 802.11b menggunakan data rate 1, 2, 5.5 dan 11 Mbps, tergantung kualitas link antara peralatan klien dengan access point. Jika kualitas link jaringan menurun, maka access point akan secara otomatis menutup data rate yang tertinggi, atau dengan kata lain akan menurunkan data rate sehingga kualitas koneksi jaringan dipulihkan. Anda juga dapat membatasinya pada data rate tertentu. Misal, jika Anda hanya ingin berkomunikasi pada



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

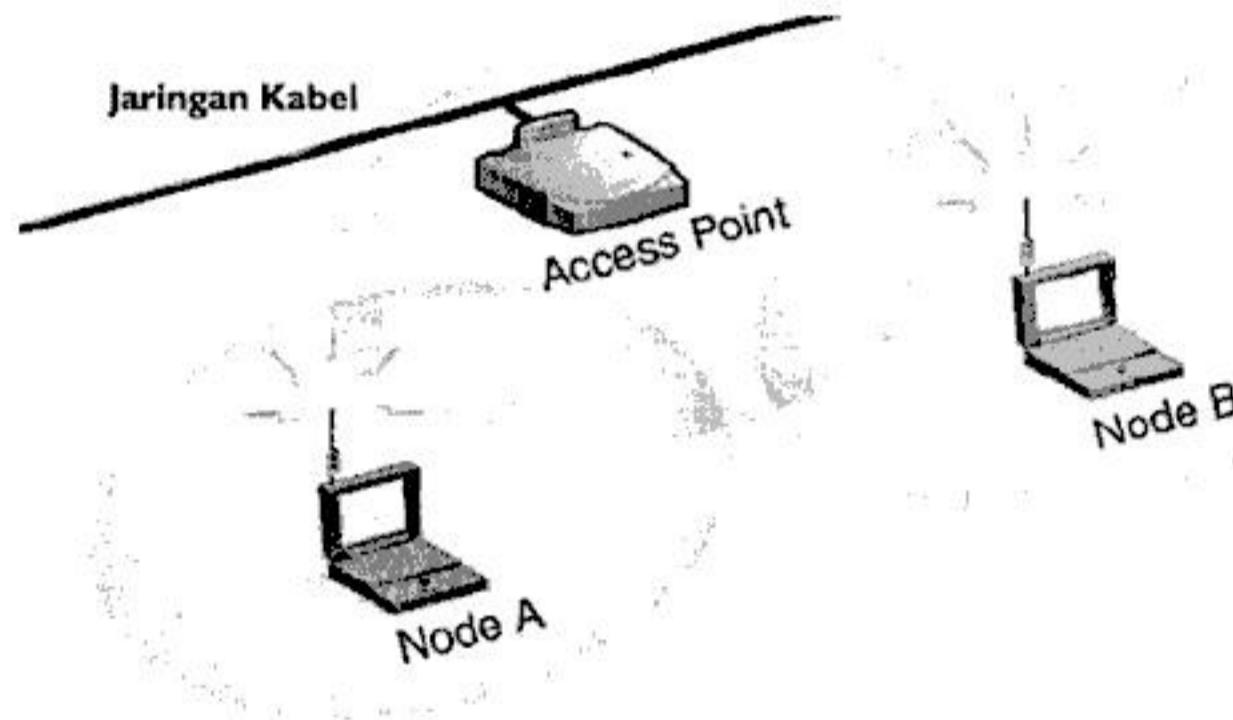


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Proksi ini bertindak sebagai access point atau base station dalam sebuah jaringan yang kompleks. Topologi Ad Hoc sangat murah diterapkan dan sangat efektif serta mudah dalam pembangunan lingkungan wireless-nya, seperti pada ruangan konferensi, kelas, atau bahkan lingkungan kerja yang relatif kecil.

3.6.2 Basic Service Set (BSS)

Topologi yang lebih kompleks adalah topologi infrastruktur, di mana paling sedikit ada satu access point yang bertindak sebagai base station. Access point akan menyediakan fungsi sinkronisasi dan koordinasi, melakukan forwarding serta broadcasting paket data. Fungsi ini hampir sama dengan teknologi bridge pada metode jaringan wired (dengan kabel).



Gambar 3-24 Topologi Basic Service Set (BSS)

3.6.3 Extended Service Set (ESS)

Pada topologi ini, beberapa access point dapat digunakan untuk meng-cover range area yang lebih luas, sehingga membentuk extended service set (ESS). Metode ini terdiri dari dua atau lebih basic service set yang terkoneksi pada satu jaringan kabel. Setiap access point diatur dalam channel yang berlainan untuk menghindari terjadinya interferensi. Metode ini akan membentuk sel-sel seperti pada jaringan selular. User dapat melakukan roaming ke sel yang lain dengan cukup mudah tanpa kehilangan sinyal.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Frame Probe Response: Station akan merespons dengan frame ini dengan menyertakan kapabilitas informasi dan dukungan data rate setelah menerima frame probe request.

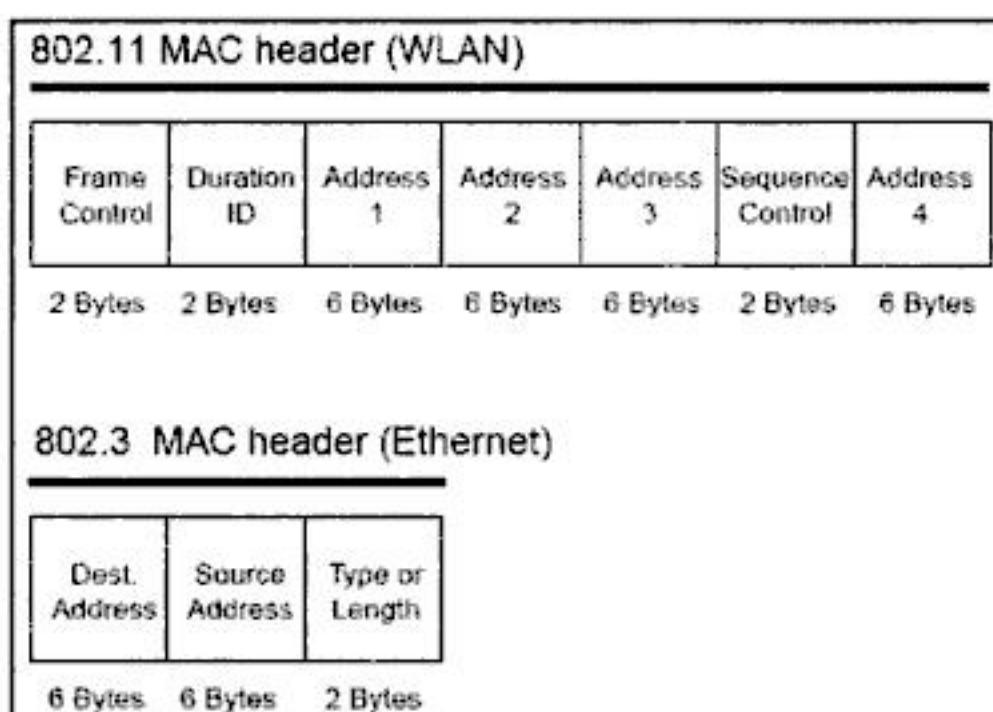
4.1.3 Struktur Paket

Semua fungsionalitas protokol terlihat pada header setiap paket. Teknologi frekuensi radio (RF) dibutuhkan untuk melakukan komunikasi dengan mobilitas yang tinggi, sehingga kebutuhannya menjadi sangat kompleks pada standar jaringan WLAN 802.11. Kerumitan ini terlihat pada header yang cukup panjang di physical layer convergence protocol (PLCP) dibandingkan pada header MAC.

OSI Physical (PHY) layer	OSI Data Link layer	higher OSI layers	packet trailer
PLCP preamble header	MAC Header	LLC (opt)	Network Data FCS End Delimiter

Gambar 4-4 Struktur Paket 802.11

Karena standar WLAN 802.11 mempunyai transmisi radio yang selalu berubah, koordinasi di antara perangkat jaringan wireless ini menjadi sangat rumit. Pengaturan paket serta manajemennya akan terdedikasi untuk membentuk suatu koordinasi fungsi yang saling mendukung. Sebagai contoh, perbandingan antara header paket data WLAN dan header paket data ethernet pada gambar Gambar 4-5.



Gambar 4-5 Perbandingan Header MAC pada WLAN dan Ethernet



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

pembicaraan. Akibatnya kemungkinan untuk berbicara menjadi besar, sehingga forum tersebut akan menjadi ramai yang menyebabkan arus lalu lintas informasi menjadi drop. Untuk itu, diperlukan seorang moderator (PCF) untuk mengatur kapan seseorang dapat berbicara dan kapan saat orang lain angkat bicara, sehingga tidak terjadi tabrakan waktu bicara (collision).

Spesifikasi layer MAC 802.11 sama dengan standar pada ethernet 802.3 wired line. Protokol 802.11 menggunakan skema CSMA/CA atau carrier sense, multiple access, dan collision avoidance. Protokol ini menggunakan algoritma tertentu untuk mendeteksi dan menghindari tabrakan, seperti pada ethernet 802.3 yang menggunakan CSMA/CD. Kita menggunakan skema collision avoidance (CA) untuk melakukan proses collision detect (CD) karena hal tersebut sangat sulit dilakukan pada frekuensi radio. MAC sublayer ini beroperasi bersama dengan layer fisik saat menggunakan media transmisi data. Layer fisik menggunakan algoritma clear channel assessment (CCA) untuk mengetahui apakah channel tersebut sedang digunakan atau tidak. Metode ini akan mengukur kekuatan energi frekuensi radio di antena dan menentukan kekuatan dari sinyal yang diterima. Jika kekuatan sinyal yang diterima di bawah ambang batas yang ditentukan, maka channel tersebut dianggap bersih, sehingga layer MAC akan memberikan status bersih untuk melakukan transmisi data. Untuk meminimalkan terjadinya tabrakan, protokol CSMA/CA menggunakan transmisi frame request to send (RTS), clear to send (CTS), dan acknowledge (ACK).

4.2.3 Proses Komunikasi

Proses komunikasi pada metode wireless mempunyai mekanisme dasar yang hampir sama dengan metode komunikasi pada sistem wired. Komunikasi akan terjadi saat sebuah node wireless mengirimkan pesan pendek berbentuk frame RTS. Pada frame RTS juga disertakan tujuan pesan dan panjang pesan. Durasi pesan ini disebut **Network Allocation Vector** (NAV). NAV akan memberikan tanda ke media untuk memberikan alokasi durasi transmisi. Station penerima akan mengirimkan kembali jawaban dalam bentuk frame CTS, yang akan berupa echoes ke pengirim dan NAV. Jika frame CTS ini tidak dikirimkan, maka diasumsikan terjadi tabrakan dan RTS akan diulang kembali. Setelah frame data



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Association: Saat autentikasi, NIC radio harus bergabung (associate) terlebih dahulu dengan access point sebelum mengirimkan frame data. Penggabungan atau association ini memerlukan sinkronisasi NIC radio dengan access point tentang beberapa informasi yang penting seperti data rate. NIC radio akan memulai association dengan mengirimkan association request frame yang berisi elemen-elemen seperti SSID dengan data rate. Access point akan merespons dengan mengirimkan association response frame yang berisi ID penggabungan tersebut dengan beberapa informasi yang diperlukan oleh access point. Setelah itu, NIC radio dan access point akan menyelesaikan proses tersebut, kemudian proses selanjutnya adalah melakukan pertukaran frame data satu dengan yang lain.

WEP: Secara optional WEP dapat diaktifkan, sehingga NIC wireless akan melakukan enkripsi body frame (tidak mengenkripsi header) sebelum melakukan transmisi menggunakan kunci yang umum, dan station penerima akan melakukan dekripsi frame berdasarkan penanda kunci umum tersebut. Standar 802.11 menggunakan kunci 40 bit, di mana kunci memudahkan orang lain untuk menyadap LAN, sehingga kurang aman. Komite 802.11i akhirnya memperbaiki standar keamanan 802.11 dengan menambahkan standar baru yang lebih aman dengan penggabungan standar 802.1X.

RTS/CTS: Fungsi dari request to send dan clear to send (RTS/CTS) adalah mengizinkan access point untuk mengatur penggunaan media pada station yang mengaktifkan RTS/CTS. Pada beberapa NIC radio, user dapat mengatur panjang ambang batas frame secara maksimum di mana NIC radio tersebut mengaktifkan RTS/CTS. Sebagai contoh, panjang frame 1.000 byte akan memicu frame RTS/CTS lebih besar dari 1.000 byte. RTS/CTS digunakan untuk mengurangi permasalahan hidden node, di mana dua atau lebih NIC radio tidak dapat mendengar satu sama lain walaupun dalam satu gabungan dengan access point yang sama.

Jika NIC radio mengaktifkan RTS/CTS, pertama-tama ia akan mengirimkan frame RTS ke access point sebelum mengirimkan frame data. Access point akan merespons dengan frame CTS yang mengindikasikan bahwa NIC radio dapat melakukan pengiriman frame data. Dengan frame CTS, access point akan menyediakan sebuah nilai field durasi dari header frame yang akan mengikat station lain untuk melakukan transmisi hingga setelah



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

jaringan yang melakukan transmisi, maka station akan mencoba melakukan transmisi dan mendengarkan apakah masih ada station lain yang melakukan transmisi data pada saat yang sama. Jika salah satu station juga melakukan transmisi data pada saat yang sama, maka akan terjadi tabrakan. Kedua pengirim data tersebut akan menarik transmisinya dan tidak akan melakukan transmisi dalam jangka waktu random.

Setelah itu, kedua station tersebut melakukan pengiriman transmisi ulang kembali, yang disebut proses 'collision detection'. Bagian 'multiple access' adalah bagian di mana lebih dari satu station dapat berada dalam satu jaringan pada waktu yang sama. Metode CSMA/CD digunakan pada ethernet atau pada jaringan wireless.

4.4.2 Token Passing

Metode media akses ini menggunakan paket khusus yang disebut token. Saat pertama kali komputer dihidupkan, saat itu pula komputer tersebut membuat token yang akan dilewatkan ke komputer lain. Token tersebut akan terus melintas ke seluruh jaringan hingga komputer yang menjadi tujuan pengiriman data menerimanya. Setiap station yang berada pada jaringan tersebut akan menerima dan membaca data yang dikirimkan serta membaca pula alamat tujuan pengiriman. Jika alamat tujuan ternyata tidak sesuai, maka station akan melepaskannya ke jaringan kembali.

Saat station mengenali alamat yang menjadi tujuan pengiriman data, NIC akan menyalin data tersebut ke memory station, kemudian melakukan modifikasi token untuk mengindikasikan bahwa data tersebut telah diterima. Token akan dikirimkan kembali ke jaringan hingga si pengirim awal menerimanya kembali. Jika data yang dikirimkan mempunyai lebih dari satu tujuan, proses akan berjalan dengan sendirinya. Jika tidak, pengirim akan memodifikasi token tersebut untuk mengindikasikan bahwa token tersebut 'bebas', artinya dapat diterima oleh siapa pun. Dengan metode token seperti ini, tabrakan tidak akan terjadi karena setiap station mempunyai hak untuk melakukan transmisi dan menerima data.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5.1.1 Pengalamatan pada Layer Network

Hubungan antara alamat network dan peralatannya hanyalah merupakan logical dan tidak fix, yang didasarkan pada karakteristik jaringan fisik atau hanya berdasarkan grup tanpa dasar fisik. End system membutuhkan satu alamat network per koneksi jaringan fisiknya pada setiap protokol layer jaringan yang didukungnya.

Alamat pada metode IPX menggunakan delapan digit heksadesimal pada bagian network. Nomor ini disebut *IPX network address*, yang diberikan secara random saat menginstal program atau dapat pula dilakukan secara manual oleh administrator jaringan. Sementara itu, bagian nodenya terdiri dari 12 digit heksadesimal alamat MAC yang diberikan oleh pabrikan. Titik dua digunakan sebagai pembatas dua bagian. Contoh alamat IPX adalah:

Alamat Network	Alamat Node
012344567:06A07C12FB89	

Gambar 5-1 Contoh Alamat IPX

Alamat TCP/IP menggunakan titik sebagai pemisah notasinya, sehingga mempunyai format xxx.xxx.xxx.xxx, sebagai contoh adalah:

192.168.0.224	Alamat IP
255.255.255.0	Subnet Mask

Alamat IP tersebut terdiri dari empat bagian yang dipisahkan dengan tanda titik. Setiap angka desimal pada alamat IP tersebut terdiri dari angka 1 hingga 254.

5.1.2 Alamat Hierarki dan Alamat Flat

Bentuk alamat internetwork terdiri dari dua buah bentuk form, yaitu *hierarchical address space* dan *flat address space*. Bentuk alamat hierarki diatur ke dalam beberapa grup besar, sedangkan pada metode alamat flat bentuk alamat diatur dalam sebuah grup.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

implementasi yang tidak benar. Router dapat mengalami kerusakan yang fatal karena diletakkan pada persimpangan-persimpangan titik jaringan. Algoritma routing yang baik harus dapat bertahan dalam serangkaian waktu tertentu dan harus stabil pada berbagai variasi bentuk jaringan.

Algoritma routing harus dapat berkonvergensi dengan cepat. Konvergensi adalah proses kesepakatan oleh semua router untuk mencapai rute yang optimal. Saat event tertentu di jaringan tidak tersedia atau tersedia, router akan mendistribusikan pesan update routing pada keseluruhan jaringan dan akan menstimulasi perhitungan ulang untuk mencapai rute yang optimal. Algoritma routing yang terlalu lambat akan menyebabkan terjadinya loop routing.

Algoritma routing harus mempunyai sifat fleksibel, artinya algoritma tersebut harus cepat dan akurat dalam beradaptasi pada lingkungan jaringan yang beragam. Sebagai contoh, dalam sebuah segmen jaringan temyata terjadi down. Untuk itu, algoritma routing harus dapat dengan cepat memilihkan jalur lain yang terbaik hingga segmen yang putus tersebut normal kembali. Algoritma routing dapat diprogram untuk melakukan adaptasi perubahan bandwith jaringan, ukuran antrean router, dan jeda jaringan antar-beberapa variabel.

Tipe-Tipe Algoritma

Tipe-tipe algoritma dapat diklasifikasikan sebagai berikut:

- ❖ Statis dan dinamis
- ❖ Jalur tunggal dan jalur banyak
- ❖ Flat dan hierarkis
- ❖ Host intelligent dan router intelligent
- ❖ Intradomain dan interdomain
- ❖ Link state dan distance vector

Statis dan Dinamis

Algoritma routing statis tidak semuanya berupa algoritma, akan tetapi juga berupa tabel pemetaan yang dapat dibuat oleh administrator jaringan. Pemetaan jaringan ini tidak akan berubah selama administrator tidak



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

IPSec merupakan protokol keamanan standar yang menyediakan metode standar dan dapat diperluas agar dapat digunakan pada layer network (IP) dan layer protokol di atasnya seperti TCP dan UDP. IPSec dapat digunakan secara ekstensif untuk keamanan koneksi jaringan dari host jaringan hingga IPSec gateway dan host yang lain. IPSec dapat pula digunakan pada entitas jaringan seperti router dan IPSec gateway.

IPSec sangat dikenal dan mempunyai mekanisme yang luas dalam penyediaan keamanan jaringan antara beberapa elemen jaringan wired, akan tetapi tidak didesain untuk memproteksi protokol layer di bawahnya seperti 802.11.

5.7 Pertanyaan

1. Apakah tanggung jawab dari layer network dan apakah yang Anda ketahui tentang routing?
2. Apakah yang Anda ketahui tentang alamat fisik dan alamat logika jaringan?
3. Apakah keuntungan dan kerugian dari alamat yang dibentuk secara hierarki dan alamat yang dibentuk secara flat?
4. Bagaimanakah konsep kerja sebuah router?
5. Bagaimanakah tabel routing dapat terbentuk dan apa fungsinya?
6. Sebutkan infomasi yang didapat dari tabel routing dan jelaskan masing-masing?
7. Apakah tujuan dari algoritma routing?
8. Sebutkan tipe-tipe algoritma routing yang Anda ketahui.
9. Apakah yang dimaksud dengan routed protocol dan routing protocol? Sebutkan contohnya.
10. Apakah yang dibutuhkan dalam melakukan pengukuran routing?
11. Apakah perbedaan antara router dan brouter?
12. Sebutkan salah satu teknik routing pada wireless network. Sebutkan keunggulan dan kelemahannya.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Tipe	Cakupan	Performa	Standar	Metode
PAN	Perorangan	Sedang	Bluetooth, 802.15, dan IrDA	Menggantikan kabel
LAN	Dalam gedung	Tinggi	802.11, Wi-Fi	Ekstensi dari jaringan kabel
MAN	Kota/kawasan	Tinggi	802.16, WIMAX	Fixed wireless
WAN	Negara/dunia	Rendah	Cellular 1G, 2G, 2.5 G, 3 G – Next G	Mobile

Sumber: *Wireless Network Firs Step*, Jim Geier

6.1 Personal Area Network

Jaringan personal mempunyai cakupan area yang sangat sempit, yaitu sekitar 20 m. Jaringan ini hanya dapat digunakan sebagai jaringan personal dalam ruangan kecil karena jaraknya yang demikian kecil. Performa jaringan wireless PAN termasuk dalam kategori sedang, di mana data rate-nya mencapai 2 Mbps.

Pemanfaatan jaringan personal wireless telah cukup luas, terutama pada peralatan-peralatan mobile seperti PDA, laptop, dan telepon selular. Beberapa bentuk pemanfaatan jaringan area kecil yang paling umum adalah aktivitas sinkronisasi antarperalatan *Gadget* dengan PC atau laptop. Bahkan beberapa peralatan mobile tersebut dapat melakukan koneksi ke printer atau peralatan multimedia yang lain, sehingga praktis dapat menggantikan komunikasi kabel tradisional.

Beberapa peralatan mobile yang dapat memanfaatkan komunikasi area kecil hanya mengonsumsi daya cukup rendah. Konsumsi daya yang rendah mengakibatkan peralatan tersebut dapat mempunyai kemampuan operasional relatif panjang tanpa harus kehilangan daya baterai atau catu dayanya.

Implementasi wireless PAN sangat ambisius diterapkan pada peralatan gadget, seperti telepon selular, PDA atau PDA Phone, audio headset, dan masih banyak lagi. Dengan headset contohnya, pengguna gadget akan dengan mudah melakukan pembicaraan dan mendengarkan musik tanpa terbebani kabel yang membelit peralatannya. Peralatan-peralatan audio visual pada PDA telah dilengkapi pula dengan berbagai peralatan nonkabel dengan cakupan lebih luas.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

PDA, terdapat tiga sistem operasi utama pada PDA, yaitu Palm OS dari Palm Incorporated, EPOC dari Symbian, dan Windows CE dari Microsoft. Semuanya menggunakan protokol IrDA untuk melakukan link dengan komputer.

6.1.3 Bluetooth

Bluetooth merupakan hasil kesepakatan beberapa perusahaan besar di dunia, seperti Ericsson, IBM, Intel, Nokia, dan Toshiba, dan diperkenalkan pada tahun 1998. Bluetooth sangat ideal untuk diterapkan pada peralatan kecil portabel dengan range jangkauan cukup dekat, dengan daya cukup kecil, dan murah. Berbagai fitur tersebut menjadikan bluetooth sebagai alternatif pengganti untuk melakukan koneksi peralatan kecil dengan area cakupan yang sangat pendek. Dalam perkembangannya, bluetooth menjadi rival berat pengembangan IrDA yang dibahas pada bab sebelumnya.

Bluetooth beroperasi hingga data rate 1 Mbps pada frekuensi 2,4 GHz dan menggunakan teknologi FHSS dengan hop pada keseluruhan spektrum berkisar 1.600 hop per detik, lebih cepat dibandingkan dengan versi frequency hopping standar 802.11. Peralatan bluetooth dengan daya yang rendah dapat mencakup range hingga 10 m, sedangkan peralatan bluetooth dengan daya yang paling tinggi saat ini telah mencapai 100 m, walaupun penerapannya masih sangat jarang. Dari segi bentuk fisik, peralatan bluetooth mempunyai form factor yang sangat kecil dengan ukuran hanya 10,2 x 14 x 1,6 mm, sehingga peralatan ini dapat diimplementasikan pada berbagai peralatan lain.

Bluetooth dapat membentuk jaringan yang paling kecil, atau disebut *piconet*, dengan 7 klien dan 1 master. Kumpulan dari piconet akan membentuk *scatter net*. Berdasarkan kemampuan tersebut, bluetooth dapat digunakan dengan berbagai variasi di dalam peralatan-peralatan mobile seperti headset, Internet bridge, dan operasi wireless lain seperti pertukaran data, sinkronisasi data, dan pencetakan. Spesifikasi bluetooth telah mencapai versi 1.1 yang dikembangkan oleh Bluetooth Special Interest Group (SIG).

Bluetooth SIG inilah yang telah mem-published spesifikasi bluetooth. IEEE telah membentuk working group 802.15 yang mendefinisikan standar untuk wireless PAN. Standar 802.15.1 untuk WPAN dibuat setelah



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

intranet, aktivitas e-mail, dan aktivitas jaringan lain. Peralatan yang digunakan tidak terbatas hanya Personal Computer atau laptop, akan tetapi peralatan mobile yang lain seperti PDA, telepon selular, notebook, atau peralatan game online lainnya.

Beberapa komponen dalam hotspot adalah:

- Station yang mobile
- Access Point
- Switch, Router, Network Access Controller
- Web server atau server yang lain
- Koneksi Internet kecepatan tinggi
- Internet Service Provider
- Wireless ISP

Hal yang perlu dipahami dalam membangun sebuah kawasan wireless area adalah konfigurasi serta persyaratan apa yang harus dipenuhi serta untuk siapa wireless area ini diperlukan. Beberapa hal tersebut adalah ukuran lokasi cakupan, jumlah perkiraan user yang simultan, dan tipe pengguna wireless sasaran. Anda dapat mempelajari secara singkat pembangunan hotspot dengan sederhana pada bagian akhir buku ini.

Ukuran lokasi cakupan: Ukuran ini menjadi pertimbangan awal yang sangat menentukan dalam membangun area wireless hotspot. Dengan menentukan lokasi cakupan, akan dapat dipilih peralatan access point (AP) mana yang dapat melayaninya, misalnya dengan menentukan daya jangkau jarak tertentu. Beberapa AP diperlukan untuk menyediakan area cakupan yang lebih luas.

Jumlah Pengguna: Dalam melakukan layout hotspot, jumlah user dapat digunakan untuk menentukan serta memerikirakan kepadatan pengguna pada kawasan tersebut. Kepadatan ini dapat diukur dari jumlah pengguna per kawasan. Di samping jumlah pengguna, hal yang lebih penting adalah pola pengguna sasaran yang dituju, sehingga akan dapat ditentukan pula target minimum bandwidth per user yang aktif. Sebagai contoh, target bandwidth adalah 100 Kbps per user aktif, di dalam daerah tersebut terkoneksi 5 user yang aktif sehingga memerlukan minimal 500 Kbps atau lebih untuk melakukan koneksi Internet dengan baik.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

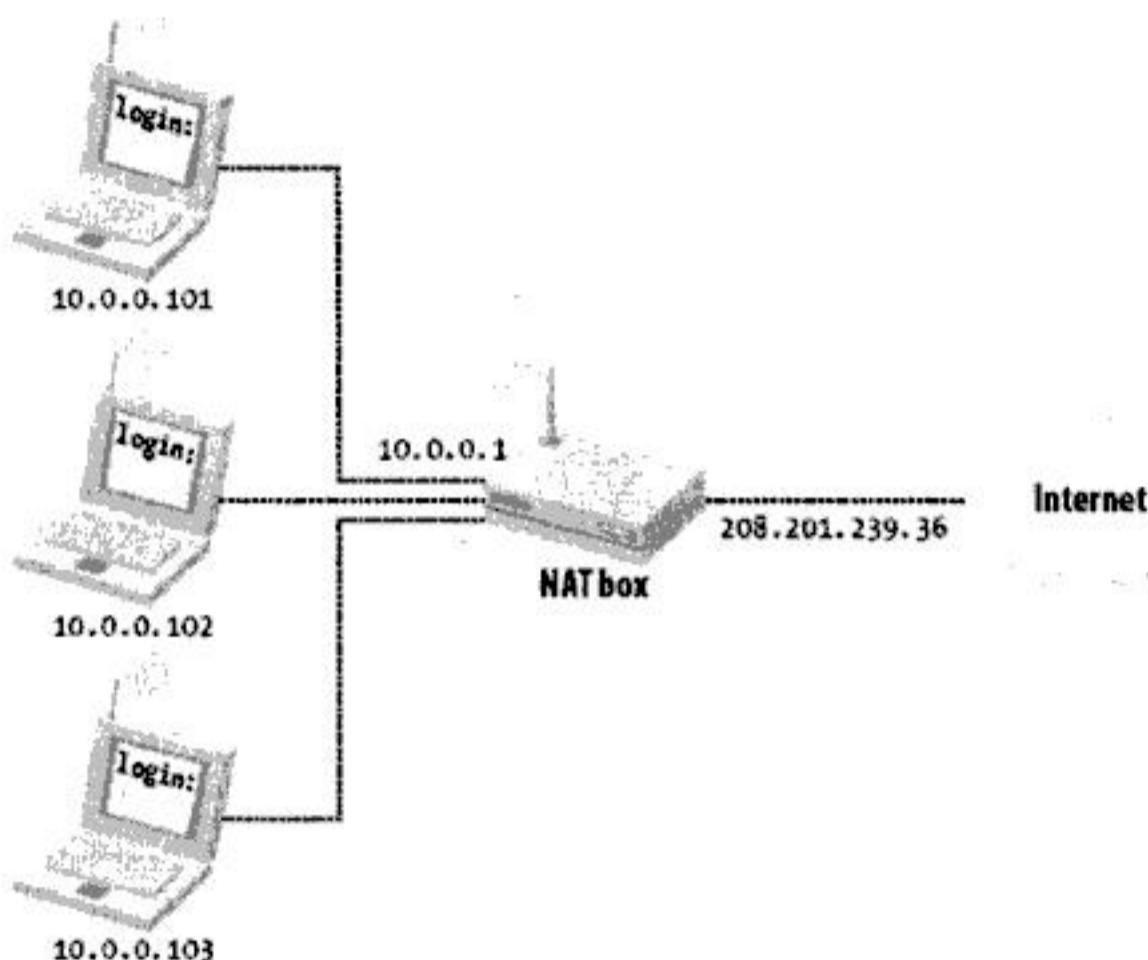


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Setiap paket tersebut akan melintas dari jaringan privat, kemudian ke jaringan publik untuk mendapatkan akses ke jaringan Internet, sehingga alamat IP sumber harus diubah ke alamat IP publik. Translasi dari alamat privat ke alamat publik ditangani oleh Network Address Translator (NAT).



Sumber: Building Wireless Community Network, O'Reilly

Gambar 6-8 Beberapa Komputer 'share' IP Address Tunggal

Variasi dari model translasi ini juga melakukan translasi port IP, peralatan ini disebut Network Address Port Translators (NAPT). Peralatan NAPT akan melakukan map atau pemetaan terhadap semua alamat IP privat ke dalam sebuah alamat IP publik.

6.3 Metropolitan Area Network

6.3.1 Wireless MAN

MAN adalah Metropolitan Area Network, yaitu jaringan yang mempunyai cakupan yang relatif luas dibanding cakupan LAN. Jaringan ini menyediakan interkoneksi outdoor dalam kawasan perkotaan atau antar gedung. Wireless MAN dipilih karena tidak begitu membutuhkan biaya yang besar jika dibandingkan jaringan melalui kabel tembaga atau melalui kabel serat optik.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

gunakan sebuah tower BTS untuk mendistribusikan sistem dalam bentuk sel-sel. Wireless LAN dengan 3G dapat menjadi sistem pelengkap satu dengan yang lain. Tantangannya ialah harus membuat standarisasi integrasi 3G dan wireless LAN untuk kemudahan dalam penggunaannya. Pengguna saat di luar batas jangkauan LAN akan dapat berasosiasi (bergabung) dengan layanan sistem selular dengan mudah, demikian juga sebaliknya. Hal yang lebih penting dari beberapa teknologi ini adalah konvergensi, di mana semua peralatan akan mempunyai standar yang sama, sehingga akan mempermudah pengguna dalam memanfaatkan semua fitur tersebut.

6.4.3.4 Selular Generasi Selanjutnya

Saat ini, pengembang software sedang mencoba mengembangkan aplikasi yang didesain untuk dapat bekerja dengan baik pada generasi ke-3 (3G) teknologi komunikasi wireless dan teknologi yang baru, yaitu generasi ke-4 (4G). Teknologi baru ini akan dapat mengembangkan aplikasi multimedia ponsel mobile, yaitu mengombinasikan antara kamera, video kamera, komputer, stereo, dan radio.

Penelitian dan pengembangan base station digital dengan bentuk ukuran fisik yang semakin mengecil dan peralatan-peralatan terminal yang telah diperbaiki teknologinya akan memperbaiki kualitas suara dan konsumsi daya, sehingga akan memperpanjang usia hidup baterai dan semakin kecilnya bentuk handset. Perkembangan aplikasi software, content, dan teknologinya akan menjadikan aplikasi mobile dapat melakukan koneksi Internet untuk mengirim permintaan data, check e-mail, dan mengirimkan fax. Beberapa ponsel mendukung software PDA yang menawarkan aplikasi kalender, address book, calculator, dan voice recorder.

Perlengkapan handset akan dilengkapi dengan software pengenal suara (voice recognition), sehingga akan mengizinkan voice dialing. Mayoritas aplikasi serta isi untuk mobile wireless handset didesain untuk melayani para pelaku bisnis yang cenderung mobile. Aplikasi-aplikasi dan isi saat ini sedang dalam tahap pengembangan, termasuk pengembangan penggunaan global positioning systems (GPS), audio dan video streaming, serta tipe-tipe aplikasi hiburan yang digunakan untuk menarik pasar.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

6.5 Pertanyaan

1. Sebutkan tipe jaringan wireless yang identik dengan jaringan wired yang Anda ketahui, dan berikan penjelasan singkat mengenai perbedaannya.
2. Apakah perbedaan metode akses antara IrDA dengan bluetooth?
3. Apakah perkembangan teknologi bluetooth akan menghabisi teknologi IrDA? Bagaimana menurut Anda?
4. Apakah bluetooth dapat menggantikan peran teknologi wireless LAN? Bagaimana menurut Anda?
5. Mengapa peralatan wireless LAN perlu disertifikasi?
6. Apakah yang Anda ketahui tentang hotspot dan komponen apakah yang diperlukan untuk membangun hotspot?
7. Apakah yang Anda ketahui dengan arsitektur mesh pada jaringan wireless?
8. Apakah yang Anda ketahui tentang WIMAX?
9. Apakah perbedaan antara pengembangan wireless MAN dengan menggunakan Wi-Fi dengan WIMAX?
10. Apakah yang Anda ketahui tentang base station pada jaringan WAN?
11. Apakah yang Anda ketahui tentang metode point to point dan metode point to multipoint?
12. Apakah yang Anda ketahui tentang istilah sel (cell) pada metode wireless WAN?
13. Jelaskan secara singkat perkembangan teknologi selular dari 1G hingga ke next G, sebutkan fitur-fiturnya.
14. Sebutkan beberapa teknik modulasi pada teknologi wireless WAN, dan sebutkan fitur-fitur standarnya.

Bab 7

Keamanan Jaringan Wireless

Wireless networks have become one of the most interesting targets for hackers today.

Saat ini, jaringan wireless menjadi target paling menarik bagi hacker.

Pemyataan di atas mengindikasikan bahwa semua aspek selalu mempunyai risiko. Ada aspek baik dan ada aspek buruk yang selalu mengikutinya. Keamanan selalu menjadi isu menarik dalam perkembangan komunikasi, interaksi, dan sosialisasi manusia. Perkembangan jaringan wireless yang begitu pesat dan populer menjadikan pihak-pihak lain yang kurang bertanggung jawab mencoba mencari celah-celah untuk dapat memanfaatkannya secara ilegal dan tidak bermaksud bagi kebaikan. Bukan mustahil bahwa saat ini jaringan wireless menjadi salah satu target penting bagi para hacker.

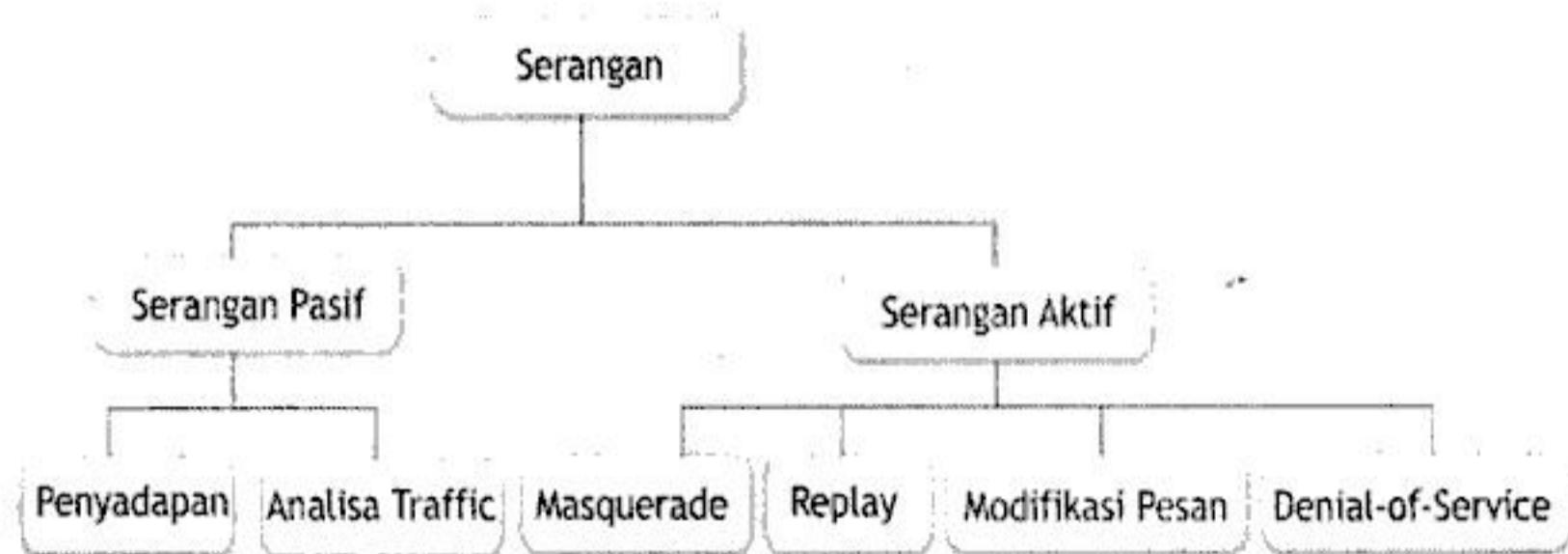
Beberapa organisasi dan perusahaan semakin gencar mengembangkan jaringan wireless karena kemudahan, kenyamanan, dan harga peralatan yang semakin terjangkau. Di pasaran, peralatan-peralatan wireless ini secara default tidak mempunyai fitur keamanan yang memadai, sehingga keberadaan peralatan wireless menjadi target utama para hacker untuk mencoba memanfaatkan berbagai kelemahannya. Hal ini didukung lagi dengan dokumen-dokumen peralatan wireless yang dengan mudah diperoleh di web site secara bebas, baik dari segi teknis detail hingga operasionalnya.

Tidak seperti pada jaringan kabel tradisional, WLAN mengirimkan datanya melalui udara bebas dan sangat memungkinkan diakses di luar batas fisik sebuah kelompok jaringan yang berhak. Sinyal komunikasi secara alami tersedia secara terbuka dan merambat melalui udara.

Saat paket data tidak dienkripsi, paket tersebut dapat dilihat oleh semua orang yang menggunakan radio frekuensi yang sama. Sebagai contoh,

seseorang memperlengkapi laptopnya dengan sistem operasi Linux, kemudian dipasang adapter WLAN agar dapat mengakses jaringan wireless. TCPDUMP dapat digunakan untuk menerima, menampilkan, dan menyimpan paket data yang bersirkulasi pada jaringan wireless.

Banyak pengembang jaringan wireless yang menyatakan bahwa WLAN mempunyai risiko keamanan yang sangat tinggi dan tidak ada jaminan keamanan yang dapat diberikan, kecuali hanya melakukan *mitigasi* risiko keamanan WLAN yang mungkin dapat dilakukan. Secara garis besar terdapat beberapa isu keamanan jaringan wireless serta risiko pengembangannya yang telah dipublikasikan, antara lain serangan terhadap kerahasiaan, integritas data, serta ketersediaan jaringan.



Sumber: Wireless Network Security, NIST

Gambar 7-1 Klasifikasi Serangan Jaringan Wireless

Serangan pasif – biasanya menggunakan akses yang bukan haknya dan tidak melakukan perubahan content atau isi paket data. Serangan pasif biasanya berupa penyadapan atau penganalisaan lalu lintas jaringan (traffic) yang sering disebut traffic flow analysis. Terdapat dua jenis serangan pasif, yaitu:

- ❖ Penyadapan atau eavesdropping, di mana penyerang melakukan pemonitoran transmisi serta isi dari pesan. Sebagai contoh, seseorang mencoba mendengarkan transmisi antara dua workstation wireless dan base station.
- ❖ Analisa traffic, penyerang menggunakan cara yang tidak dirasakan pihak yang diserang dengan menggunakan metode pemonitoran

yang lebih canggih untuk membuat pola komunikasi pihak yang diserang. Sejumlah informasi dapat dirangkai dan didapatkan melalui aliran pesan di antara bagian-bagian yang saling berkomunikasi.

Serangan aktif – penyerang yang sebenarnya tidak berhak atas akses jaringan akan melakukan modifikasi data, aliran data, atau file. Serangan ini mudah sekali dideteksi, akan tetapi tipe ini sangat sulit untuk dihindari. Serangan aktif dapat berupa kombinasi dari keempat serangan aktif, yaitu masquerading, replay, modifikasi pesan, dan DoS.

- ❖ Masquerading – penyerang akan menyamar sebagai user yang mempunyai hak untuk menggunakan jaringan, sehingga dapat memanfaatkan resource jaringan pihak yang diserang.
- ❖ Replay – penyerang akan memonitor transmisi (serangan pasif) terlebih dahulu, kemudian akan melakukan transmisi ulang pesan tersebut selayaknya user yang berhak memanfaatkan jaringan.
- ❖ Modifikasi pesan – penyerang akan mengubah pesan asli dengan cara menghapus, menambah, dan melakukan penyusunan ulang pesan.
- ❖ Denial of Service (DoS) – penyerang akan mencegah bahkan menghalangi penggunaan jaringan secara normal hingga menghalangi pengaturan fasilitas komunikasi.

7.1 Memahami Risiko

Ada tiga hal yang dapat membuat lingkungan jaringan lebih aman, yaitu dengan kontrol akses, privasi, dan autentikasi paket data.

Kontrol akses, adalah membatasi user yang dapat menggunakan jaringan. Kontrol akses merupakan metode desain autentikasi user, sehingga dapat melakukan verifikasi mengenai user mana yang berhak menggunakan sumber daya jaringan dan mana yang tidak boleh. Beberapa metode autentikasi antara lain Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP), dan Extensible Authentication Protocol (EAP).

Privasi, adalah melakukan penyembunyian informasi dari orang-orang yang tidak berhak. Transmisi jaringan wireless sangat rentan dengan kemudahan browsing data paket apabila tidak melalui proses enkripsi. Enkripsi adalah proses penyandian (encode) data, sehingga tidak akan dimengerti oleh penyadap atau orang yang tidak memahami dan berhak terhadap kunci pembacaan data. Enkripsi dapat melalui layer 2 dengan pertukaran kunci yang lebih aman (Secure Key Exchange), atau melalui layer 3 menggunakan Virtual Private Network (VPN).

Autentikasi, autentikasi adalah proses pemeriksaan peralatan user yang sah, sehingga paket yang dikirimkan benar-benar berada di tangan user yang berhak.

Meskipun Anda telah melakukan beberapa hal di atas, masih banyak peluang dan celah keamanan dalam teknologi jaringan wireless yang mungkin mendapat serangan, bahkan cenderung meningkat. Beberapa risiko keamanan tersebut antara lain:

- ❖ Serangan penyusupan.
- ❖ Pemonitoran lalu lintas jaringan oleh orang yang tidak berhak dengan melakukan bypass monitor jaringan.
- ❖ Jamming atau Denial of Service (DoS)
- ❖ Serangan client to client
- ❖ Brute force attacks pada password-password access point
- ❖ Serangan enkripsi
- ❖ Misconfiguration
- ❖ Man in the middle attack

7.1.1 Serangan Penyusupan

Pada awal bab ini telah dijelaskan bahwa sinyal komunikasi jaringan wireless tersedia secara terbuka dan merambat melalui udara, sehingga orang lain dapat mengakses jaringan dari luar dengan mudah jika tindakan pencegahan tidak dilakukan dengan benar. Dapat diibaratkan bahwa seseorang akan dapat memasuki station pusat jaringan dengan mudah di perusahaan Anda, sehingga penyusup akan dapat melakukan

akses ke server perusahaan Anda dengan leluasa, menggunakan resource jaringan internal, bahkan mengambil file-file penting perusahaan Anda.

Sangat disayangkan karena banyak perusahaan yang mengembangkan jaringan wireless-nya hanya dengan menggunakan beberapa aturan default bawaan dari pabrikan dengan konfigurasi yang cenderung standar, sehingga memungkinkan seseorang untuk dapat melakukan interface pada server aplikasi. Lebih parah lagi, pemasangan access point LAN tidak dilengkapi dengan pengaturan keamanan yang benar atau bahkan justru tidak diatur sama sekali. Akibatnya, seseorang akan dapat memanfaatkan resource jaringan tersebut dengan leluasa seperti akses hard disk, printer, dan koneksi Internet.

Penyusupan jaringan ini terbagi menjadi dua, yaitu:

Klien yang tidak berhak, si penyerang akan mencoba melakukan koneksi wireless klien, biasanya melalui laptop atau PDA ke access point tanpa autorisasi. Access point dapat dikonfigurasikan untuk memberikan password ke klien yang melakukan akses tersebut. Jika access point tidak di-password, penyusup dapat dengan mudah melakukan koneksi jaringan internal karena tanpa password berarti wireless klien diberi izin untuk melakukan komunikasi dengan access point.

Access point yang tidak berhak, biasanya sebuah perusahaan tidak memedulikan pengembangan jaringan wireless internal yang dilakukan oleh pegawainya sendiri. Ketidakpedulian inilah yang dapat memicu akses resource jaringan perusahaan oleh klien dengan memasang access point yang sesungguhnya bukan hak klien untuk memasangnya, dan ketidak tahuhan implikasi pemasang jaringan akan keamanan data internal perusahaannya. Beberapa istilah yang umum digunakan untuk menyebut access point ini adalah *Rogue Access Point* atau *Renegade Access Point*. Rogue access point akan berbahaya jika dilakukan oleh orang luar (hacker) perusahaan yang memang akan memanfaatkan jaringan internal perusahaan tersebut untuk kepentingan pribadi.

Rogue access point sangat mudah dimanfaatkan oleh hacker karena biasanya tidak dienkripsi dengan benar, sehingga menyediakan sarana terbuka bagi beberapa orang yang tidak berhak untuk menggunakan akses ke jaringan internal perusahaan tersebut. Untuk menghindari hal demikian, perusahaan seharusnya melakukan pemonitoran untuk



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



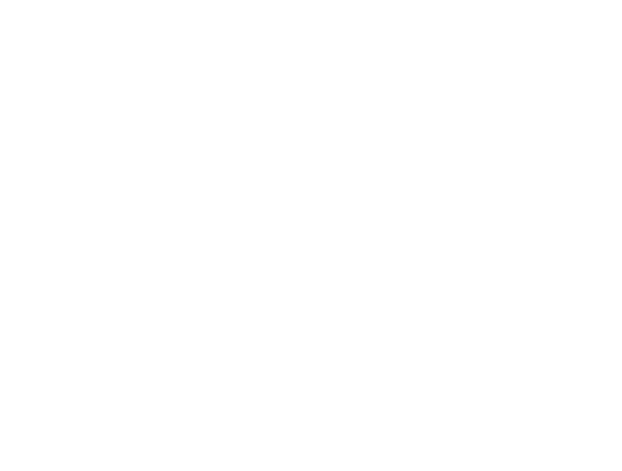
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



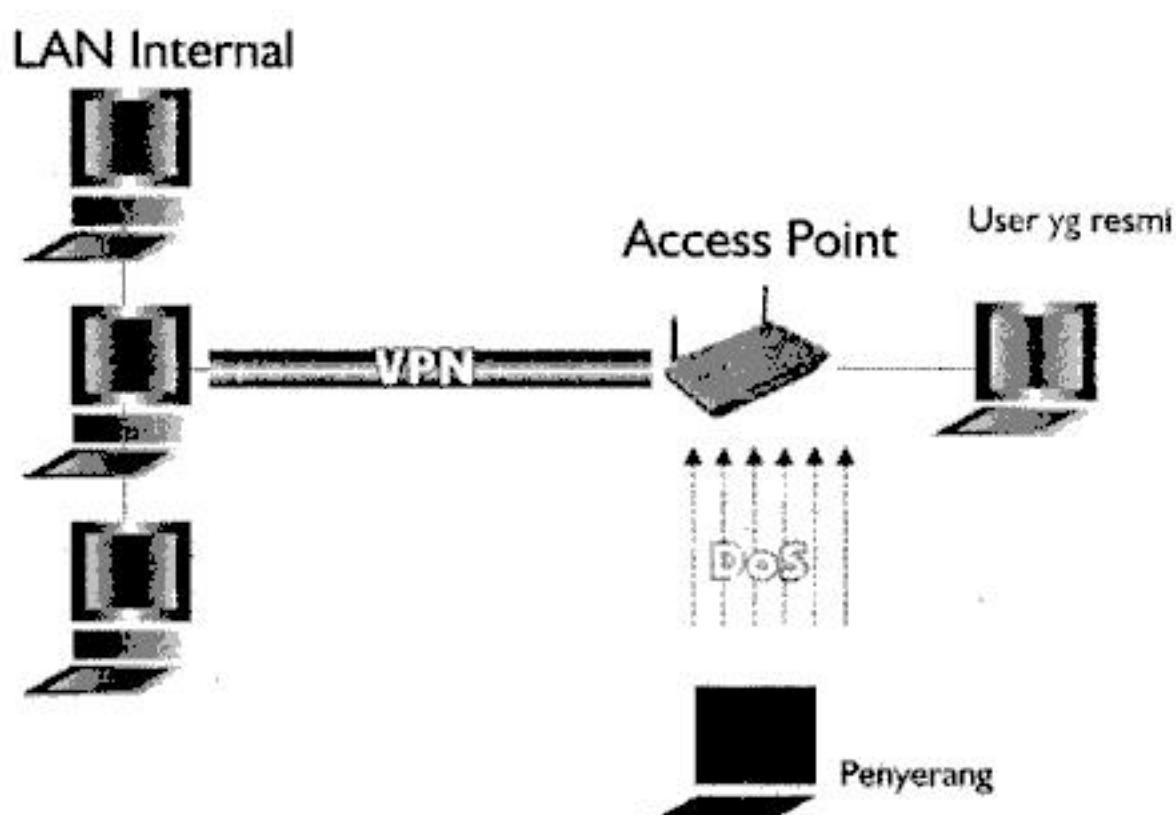
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



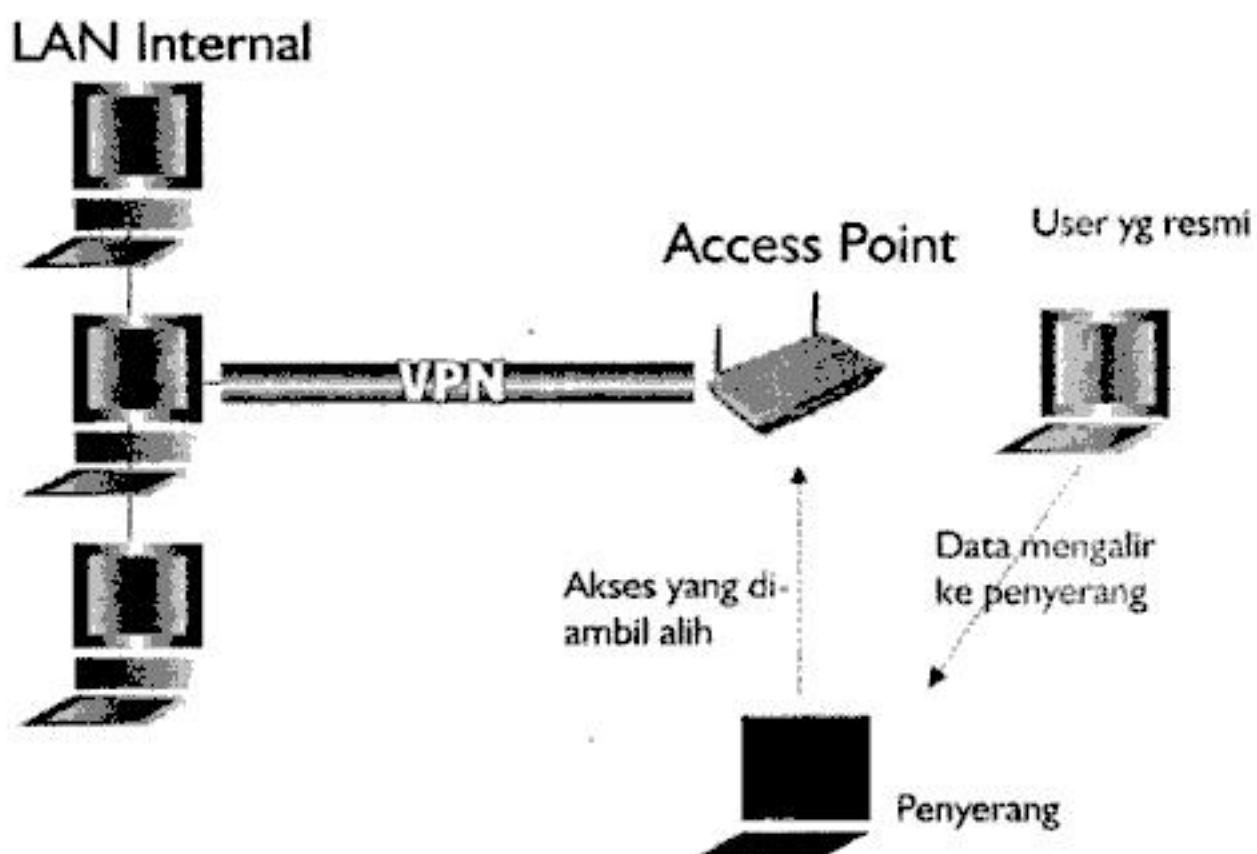
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

**Gambar 7-13 DoS**

MitM. Layer network secara khusus tidak menyediakan keamanan untuk protokol selain IP, sehingga protokol lain dapat menjadi celah keamanan yang efektif. Salah satu contoh adalah menggunakan Address Resolution Protocol (ARP). Penyerang dapat menggunakan metode serangan Man in the Middle (MitM) dengan menggunakan pesan ARP palsu untuk memasukkan entitas ke dalam alur data.

**Gambar 7-14 MitM**



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Dalam keseluruhan sistem terdapat dua jenis port, yaitu port yang dikontrol dan yang mengontrol. Port yang dikontrol hanya akan menerima paket dari sistem yang terautentikasi. Paket ini merupakan alamat MAC pada daftar alamat yang telah diautentikasi.

Aspek autentikasi pada alamat MAC merupakan dasar dari 802.1x. Tidak ada cara lain bagi autentikator dalam melakukan identifikasi, tanpa mekanisme autentikasi per paket di layer yang lebih tinggi.

Komponen ketiga adalah komponen authentication server (AS). Fungsi utama dari sistem autentikator ini adalah bertindak sebagai proksi EAP antara klien dengan access point. Paket EAP dari sisi klien akan melakukan forward paket EAP ke AS melalui protokol RADIUS.

7.4 Manajemen WLAN

Teknologi sinyal radio atau RF (Radio Frequency) sangat dinamis dan begitu ambisius dikembangkan untuk diaplikasikan pada kehidupan manusia. Banyak sekali hal yang perlu mendapat perhatian berkaitan dengan kelemahan alami dari teknologi ini. Kelemahan-kelemahan ini telah dikupas dengan cukup lengkap pada bab-bab sebelumnya, antara lain noise, interferensi, kepadatan lalu lintas, dan permasalahan kekuatan sinyal.

Saat lalu lintas jaringan menyebar melalui media yang terbuka, seperti udara, tantangan terberat adalah dalam segi keamanan serta aktivitas penyusupan yang dilakukan oleh pihak-pihak yang memanfaatkan kelemahan alami jaringan wireless ini. Pemonitoran RF diperlukan untuk menghindari hal tersebut, tentunya dengan menggunakan perkakas yang tepat.

Pendekatan umum dalam melakukan manajemen WLAN terbagi menjadi tiga, yaitu:

- ❖ Menggunakan laptop atau access point sebagai sensor background. Pada model ini laptop maupun access point dapat digunakan sebagai sensor RF dan pendekripsi paket serta mem-forward-kan paket tersebut ke software manajemen pusat. Model ini bukan merupakan sensor yang terdedikasi dan hanya berjalan pada aktivitas background.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

9. Bagaimana melakukan crack pada WEP?
10. Apakah keunggulan IPSec yang Anda ketahui?
11. Apakah yang Anda ketahui dengan server RADIUS? Apakah keunggulannya.
12. Secara garis besar, keamanan WLAN dapat diciptakan dengan melalui dua metode yaitu pencegahan dan deteksi, jelaskan dengan singkat dua metode tersebut.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



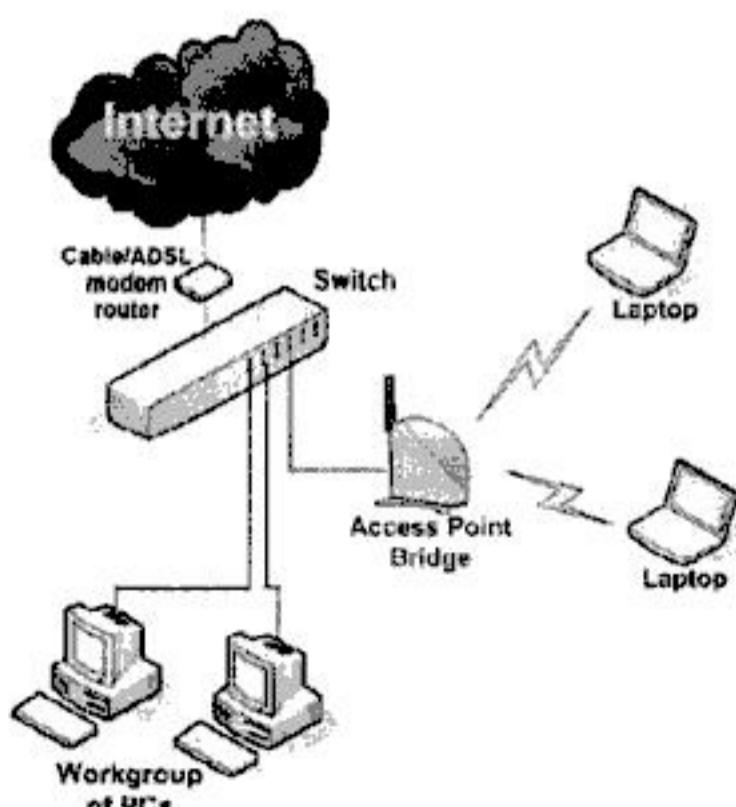
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

4. Akan sangat membantu apabila sebuah kawasan mempunyai peta dan floor plan yang cukup detail untuk membantu penempatan access point. Berikan perkiraan area cakupan pada peta serta perkiraan tipe antena untuk mencapai cakupan yang direncanakan.

Setelah Anda melakukan beberapa perencanaan, analisa, hingga perkiraan kapasitas dengan cukup detail dan mencukupi, langkah selanjutnya adalah melakukan instalasi fisik yang didasarkan pada beberapa perencanaan tersebut.

8.2 Studi Kasus Hotspot Sederhana

Bagian ini merupakan bagian terakhir dari buku ini, di mana Anda dapat menerapkan secara praktis beberapa metode pengembangan hotspot standar yang dapat Anda gunakan untuk melakukan sharing berbagai resource pada keseluruhan jaringan Anda. Penulis menggunakan access point compex WPE54G 2A serta NIC wireless adapter WLAN WLU54G 1A, dengan topologi seperti pada Gambar 8-2. Interoperabilitas access point adalah pada standar 802.11g dan 802.11b. Fungsi access point ini dapat dimanfaatkan untuk berbagai mode, antara lain sebagai access point bridging, access point client, gateway, wireless routing client, dan wireless adapter.



Sumber: User Manual, Compex WPE84G

Gambar 8-3 Topologi Fisik Hotspot



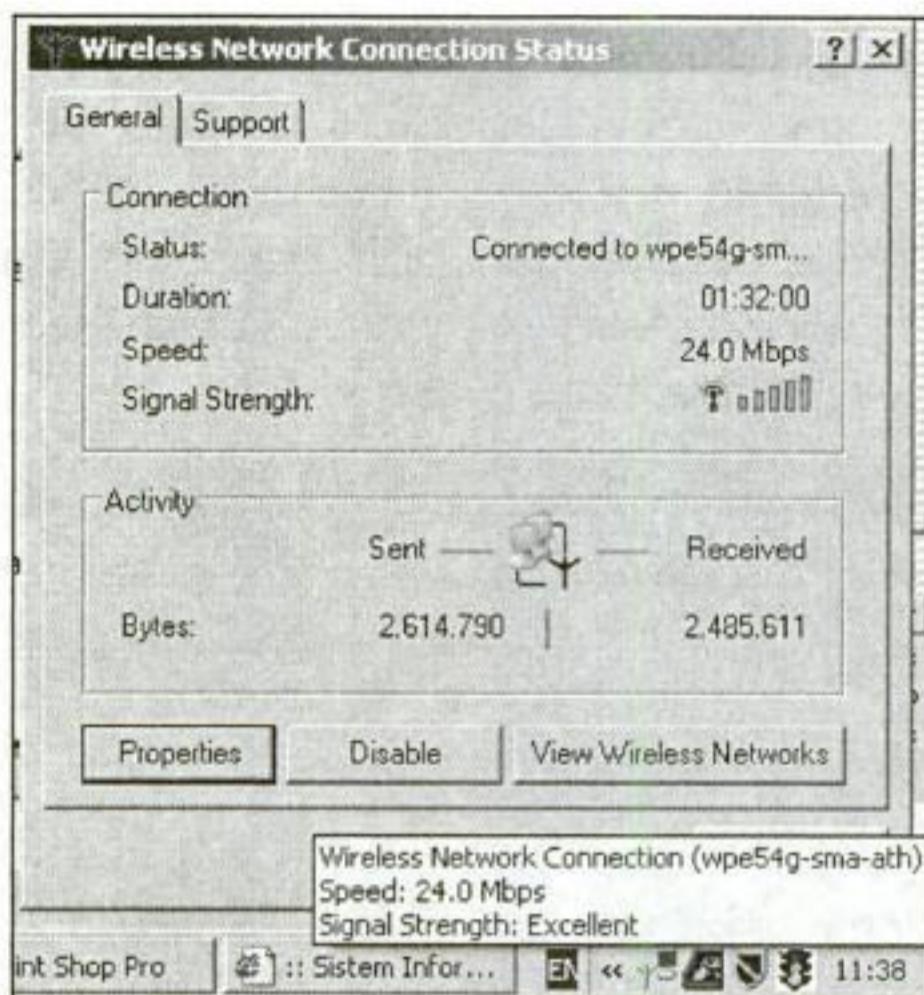
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

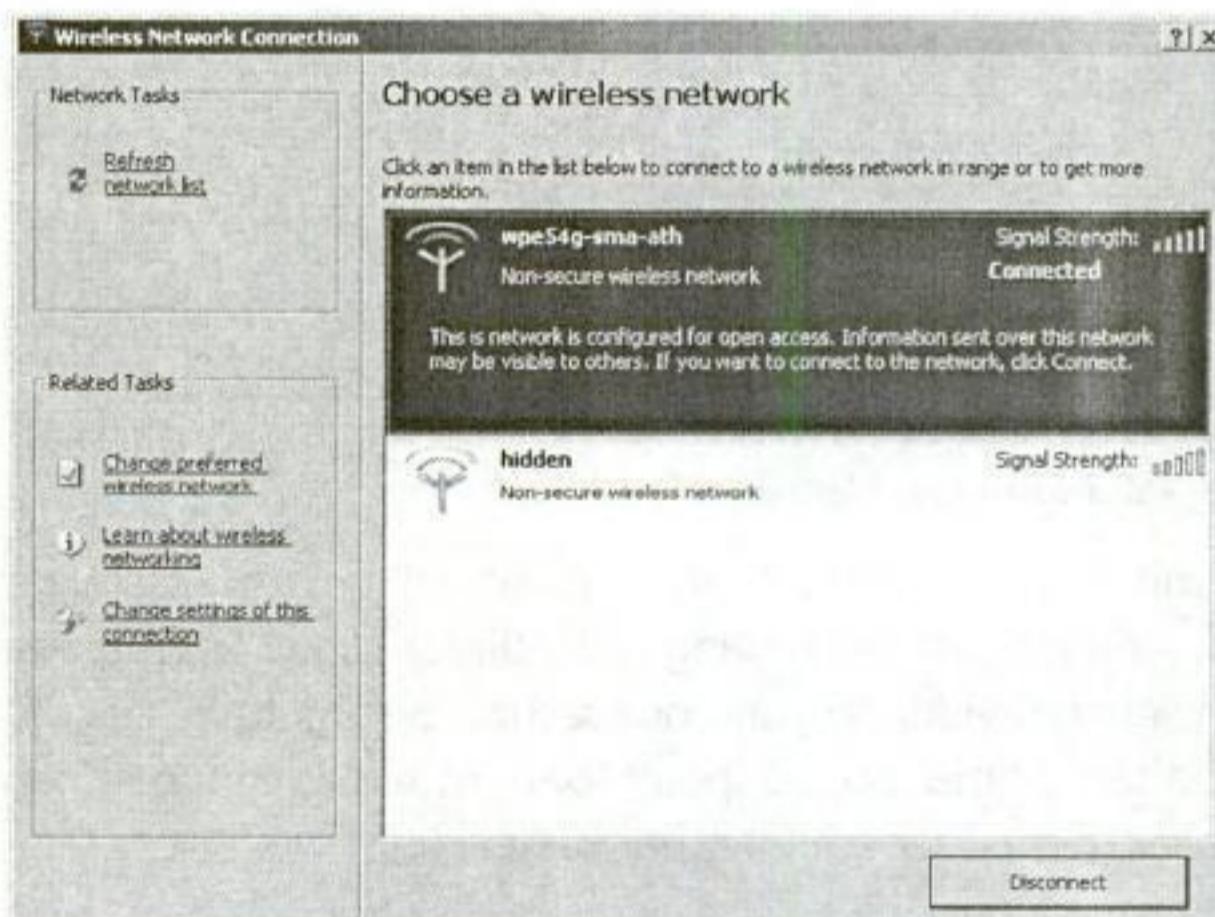


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 8-10 Sinyal Koneksi Wireless

Aturlah IP Anda sesuai dengan perencanaan IP yang ada pada jaringan internal maupun koneksi jaringan ke Internet Anda. Anda dapat pula melakukan pemeriksaan ketersediaan jaringan wireless yang tertangkap oleh NIC Anda.



Gambar 8-11 Koneksi yang Tersedia



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Digital Certificate. Pesan elektronis yang berisi mandat atau kepercayaan untuk pengguna tertentu. Digital Certificate digunakan untuk autentikasi pengguna atau peralatan komputernya.

Digital signal. Sinyal yang mempunyai tingkatan amplitudo yang bervariasi sebagai tingkatan waktu. Sinyal digital ini merepresentasikan data yang ada pada peralatan komputer. Sinyal digital harus dikonversikan terlebih dahulu ke bentuk analog (disebut modulasi) sebelum data tersebut dikirimkan melalui media udara.

Directional antenna. Adalah tipe antena yang memfokuskan gelombang radio dan rangnya dalam satu arah ke antena yang lain. Antena ini sangat umum digunakan pada wireless MAN dan WAN. Fokus langsung pada gelombang akan meningkatkan jangkauan arah pancaran gelombangnya.

DS – Distribution System. Beberapa access point yang saling terkoneksi pada jaringan wired. Atau dapat dikatakan sebagai sistem jaringan wired yang secara fisik melakukan interkoneksi access point.

DSSS – Direct Sequence Spread Spectrum. Tipe penyebaran spektrum di mana tingkatan kode penyebaran sinyal aliran data menyebar menjadi sinyal melalui bagian yang lebar pada sebuah band frekuensi. Standar jaringan wireless 802.11b menggunakan direct sequence ini.

EAP – Extensible Authentication Protocol. Protokol umum untuk autentikasi yang mendukung mekanisme beberapa autentikasi.

EAPOL – EAP Over LAN. Teknik enkapsulasi paket EAP pada lingkungan LAN.

Encryption. Pengacakan bit data sebelum data dikirimkan ke jaringan. WEP dan WPA adalah contoh enkripsi pada jaringan wireless.

ESS – Extended Service Set. Jaringan wireless yang memanfaatkan access point lebih dari satu.

Ethernet. Jaringan wired 802.3, di mana tipe ini merupakan tipe umum untuk melakukan interkoneksi antar-PC maupun dengan server.

FDMA – Frequency Division Multiple Access. Proses yang membagi secara relatif lebar band frekuensi menjadi subband yang lebih kecil, di



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Bagi Anda yang baru memasuki dunia jaringan komputer maupun jaringan komputer tanpa kabel (wireless), maka buku ini akan sangat membantu dalam mengenali berbagai hal, khususnya tata cara komunikasi (protocol) yang digunakan di jaringan komputer wireless. Buku ini membahas banyak hal dan terminologi yang berkaitan dengan jaringan komputer yang dioperasikan tanpa kabel (wireless).

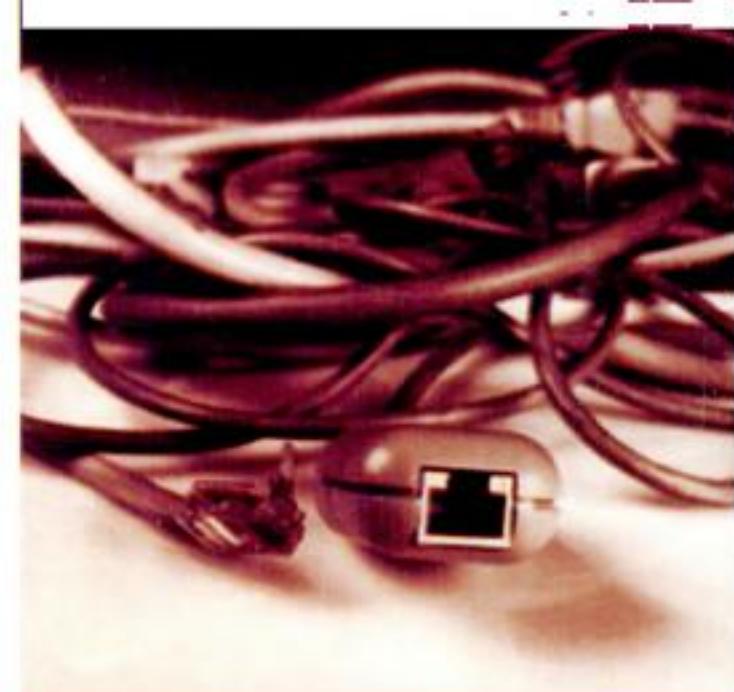
Di awali dengan pembahasan berbagai model jaringan seperti TCP/IP, Open System Interconnection (OSI) dan berbagai lapisan protocol. Pembahasan kemudian berlanjut ke konsep dasar pertukaran data di jaringan komputer, termasuk komunikasi dua arah peer to peer, komunikasi antar sistem, interaksi antar lapisan dan arsitektur jaringan wireless.

Fisik jaringan yang berbeda di jaringan wireless juga dibahas meliputi protokol yang berbasis IEEE 802, berbagai hal detail dari lapisan fisik jaringan seperti masalah channel, jarak, performance, konfigurasi ad-hoc, konfigurasi client dan access point. Beserta kemungkinan pengembangannya untuk hotspot dan berbagai bridge. Tentunya tidak kalah penting mengenali berbagai card jaringan, antenna, teknik modulasi untuk mengirimkan data kecepatan tinggi.

Semoga buku ini dapat menambah wawasan bagi mereka yang baru saja memasuki dunia jaringan komputer wireless untuk dapat mengembangkan ilmunya dengan lebih baik lagi.

Onno W. Purbo

Penulis adalah pemerhati dan praktisi Teknologi Informasi yang tinggal di Yogyakarta. Saat ini sedang menyelesaikan kuliahnya di Magister Teknologi Informasi, Universitas Gadjah Mada. Di tengah kesibukannya sebagai karyawan perusahaan swasta di Yogyakarta, dan tugas-tugas kuliah yang menumpuk, beliau masih menyempatkan menuliskan beberapa buku tentang Teknologi Informasi yang menjadi minatnya.



PENGENALAN PROTOKOL
JARINGAN
Wireless
KOMPUTER



KOMPUTER-JARINGAN

ISBN : 979-731-836-2



9 789797 318369

2 3 4 5 6 7 8 9 10