BAB II

LANDASAN TEORI

2.1 Wireless Networking

Wireless Network adalah jaringan komputer dimana koneksi pengguna dengan jaringan tersebut tidak menggunakan kabel. Komunikasi antara pengguna dengan jaringan nirkabel dilakukan melalui gelombang elektromagnetik pada frekuensi radio. Komunikasi nirkabel ini terjadi antara pengguna (Notebook, PDA, dll.) dengan suatu perangkat yang dinamakan dengan *Access Point*. *Access Point* ini yang akan menghubungkan pengguna tersebut dengan jaringan komputer yang sesungguhnya. (www.if.lib.itb.ac.id, 2005).

2.2 Wi-Fi

Merupakan kependekan dari *Wireless Fidelity*, memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (*Wireless Local Area Networks*-WLAN) yang didasari pada spesifikasi IEEE 802.11. Semua produk yang telah di test dan disetujui dengan label *Wi-Fi Certified* oleh *Wi-Fi Alliance* berarti memiliki interoperabilitas satu sama lain sekalipun berbeda jenis, merk dan vendor. Secara umum setiap produk *Wi-Fi* bekerja pada frekuensi yang sama (2,4 GHz dan 5.x GHz) dan dapat saling bekerja satu sama lain meskipun tidak tersertifikasi oleh *Wi-Fi Alliance*. Istilah *Wi-Fi* umumnya digunakan untuk teknologi berbasis standar IEEE 802.11, sebagaimana istilah *Ethernet* digunakan untuk standar IEEE 802.3. (www.id.wikipedia.org, 2007).

2.3 Wireless LAN

Adalah suatu jaringan area lokal nirkabel yang menggunakan gelombang radio sebagai media transmisinya: link terakhir yang digunakan adalah nirkabel, untuk memberi sebuah koneksi jaringan ke seluruh

pengguna dalam area sekitar. Area dapat berjarak dari ruangan tunggal ke seluruh kampus. Tulang punggung jaringan biasanya menggunakan kabel, dengan satu atau lebih titik akses jaringan menyambungkan pengguna nirkabel ke jaringan berkabel. (www.id.wikipedia.org, 2006).

2.4 Standar IEEE 802.11

Institut Of Electrical and Electronics Engineers (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*. (Edi S. Mulyanta, 2005).

Tabel 2.1 Perkembangan Standar 802.11

802.11	Standar dasar WLAN yang mendukung transmisi data 1 Mbps hingga 2 Mbps.
802.11 a	Standar High Speed WLAN untuk frekuensi 5 GHz yang mendukung transmisi data hingga 54 Mbps.
802.11 b	Standar WLAN untuk 2,4 GHz band yang mendukung transmisi data hingga 11 Mbps atau biasa di sebut Wi-fi.
802.11 e	Perbaikan dari QoS (Quality of Services) pada semua interface radio IEEE WLAN.
802.11 f	Mendefinisikan komunikasi inter-access point untuk memfasilitasi beberapa vendor yang mendistribusikan WLAN.
802.11 g	Menetapkan teknik modulasi tambahan untuk 2,4 GHz band yang dimaksudkan untuk menyediakan kecepatan hingga 54 Mbps.
802.11 h	Mendefinisikan pengaturan spektrum 5 GHz band yang digunakan di Eropa dan Asia Pasifik.
802.11 i	Menyediakan keamanan yang lebih baik. Penentuan alamat

	dimana terdapat kelemahan keamanan pada protokol autentifikasi dan enkripsi.
802.11 j	Penambahan pengalamatan pada channel 4.9 GHz hingga 5 GHz untuk standar 802.11 a di Jepang.

Standarisasi jaringan *wireless* yang digunakan di Indonesia pada umumnya adalah 802.11a, 802.11b dan 802.11g.

2.4.1 802.11a

Pada akhir 1999, IEEE mengeluarkan 802.11a yang beroperasi pada pita 5 GHz dengan menggunakan *Orthogonal Frequency Division Multiplexing* (OFDM) serta memiliki *data rate* hingga 54 Mbps. Namun sampai tahun 2000 produk ini tidak tersedia karena terdapat kesulitan dalam hal pengembangan band 5 GHz. Standar ini secara aktual mempunyai jangkauan 50 meter. *Access Point* dan *Network Interface Card* (NIC) dengan standar 802.11a mulai tersedia pada akhir tahun 2001.

Keuntungan utama dari standar 802.11a adalah kapasitasnya yang cukup tinggi yaitu mencapai 11 channel yang terpisah secara non-overlapping, yang menjadikan standar ini sebagai pilihan yang tepat untuk mendukung aplikasi yang membutuhkan performa tinggi seperti *video streaming*. Keuntungan yang lain adalah pita 5 GHz tidak begitu padat sehingga potensi terjadinya interferensi RF sangat kecil.

Kekurangan dari standar ini adalah terbatasnya cakupan range pancarannya karena menggunakan frekuensi 5 GHz, sehingga cakupan rangenya tidak lebih dari 50 meter. Akibatnya standar ini memerlukan *access point* lebih banyak. Selain itu standar 802.11a tidak kompatibel dengan standar 802.11b/g, sehingga kartu radio standar 802.11b tidak dapat bergabung dengan *access point* 802.11a.

2.4.2 802.11b

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 meter pada fasilitas dalam gedung. Range ini sangat efektif digunakan untuk pengembangan LAN secara *wireless* dibandingkan dengan standar sebelumnya.

Kekurangan saat menggunakan standar 802.11b adalah penggunaan channel pada pita 2.4 GHz dibatasi, yaitu hanya 3 buah channel. Beberapa perusahaan hanya menggunakan channel 1, 6 dan 11 untuk pemasangan *access point*, namun antara satu dengan yang lain tidak timbul interferensi. Kekurangan lain adalah terjadinya kemungkinan interferensi RF dengan peralatan radio yang lain, seperti telepon *cordless* dan *microwave*.

2.4.3 802.11g

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

Keunggulan standar ini adalah kompatibelnya dengan standar sebelumnya, yaitu standar 802.11b. Beberapa perusahaan yang telah menggunakan jaringan standar 802.11b mengupgrade *access point* mereka ke standar 802.11g dengan cara yang cukup sederhana.

2.5 Konsep TCP/IP

TCP/IP (*Transmission Control Protocol*/*Internet Protocol*) adalah sekumpulan protokol yang terdapat didalam jaringan komputer yang

digunakan untuk berkomunikasi atau bertukar data antar komputer. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak *(software)* di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah *TCP/IP stack*. (Melwin Syafrizal, 2005).

2.5.1 TCP

TCP merupakan *connection-oriented*, yang berarti bahwa kedua komputer yang ikut serta dalam pertukaran data harus melakukan hubungan terlebih dahulu sebelum pertukaran data berlangsung. TCP merupakan protokol yang bertanggung jawab untuk mengirimkan aliran data ke tujuan secara berurutan.

2.5.2 IP

IP bertanggung jawab setelah hubungan berlangsung. Tugasnya adalah merutekan paket data dalam network. IP hanya bertugas sebagai kurir TCP dan mencari jalur tebaik dalam penyampaian datagram.

2.5.3 Lapisan Protokol TCP/IP

Setiap lapisan yang dimiliki oleh kumpulan protokol TCP/IP diasosiasikan dengan protokolnya masing-masing. Protokol utama dalam protokol TCP/IP adalah sebagai berikut:

1. Protokol lapisan aplikasi: bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol *Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP)*, dan masih banyak protokol lainnya. Dalam beberapa implementasi stack protokol, seperti halnya Microsoft TCP/IP, protokol-protokol lapisan

aplikasi berinteraksi dengan menggunakan antar muka Windows Sockets (Winsock) atau NetBIOS over TCP/IP (NetBT).

2. Protokol lapisan antar-host: berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat *connection-oriented* atau *broadcast* yang bersifat *connectionless*. Protokol dalam lapisan ini adalah *Transmission Control Protocol (TCP)* dan *User Datagram Protocol (UDP)*.
3. Protokol lapisan internetwork: bertanggung jawab untuk melakukan pemetaan *(routing)* dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah *Internet Protocol (IP)*, *Address Resolution Protocol (ARP)*, *Internet Control Message Protocol (ICMP)*, dan *Internet Group Message Protocol (IGMP)*.
4. Protokol lapisan antar muka jaringan: bertanggung jawab untuk meletakkan frame-frame jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi transport, mulai dari teknologi transport dalam LAN (seperti halnya Ethernet dan Token Ring), MAN dan WAN (seperti halnya dial-up modem yang berjalan di atas *Public Switched Telephone Network (PSTN)*, *Integrated Services Digital Network (ISDN)*, serta *Asynchronous Transfer Mode (ATM)*.

2.6 Address Resolution Protocol (ARP)

Address Resolution Protocol disingkat ARP adalah sebuah protokol dalam *TCP/IP Protocol Suite* yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat *Media Access Control (MAC Address)*. ARP bertugas untuk menterjemahkan IP address ke alamat Ethernet. Penerjemahan dari IP address ke alamat *Ethernet* dilakukan dengan melihat sebuah table yang disebut cache ARP. *Entry cache* ARP berisi IP address host beserta alamat *Ethernet* untuk host tersebut. IP address

suatu host bergantung pada IP address jaringan tempat host tersebut berada, selama alamat *Ethernet* sebuah NIC bergantung pada alamat yang diberikan vendornya.

Agar dua PC dalam jaringan dapat berkomunikasi, mereka harus mengetahui *address physical machine* (MAC). Untuk membroadcast ARP, sebuah host dapat menemukan secara dinamik sebuah layer *MAC address* koresponden untuk *particular IP Network-layer address*.

Setelah menerima sebuah layer address MAC, IP devices akan membuat sebuah ARP cache untuk menyimpan sementara acquires IP-to-MAC pengalamatan address. Jika sebuah device tidak merespon bersama sebuah *specified time frame*, maka didalam entry cache akan dihapus.

Misalkan sebuah PC dengan IP Address 172.24.12.15 akan mengirim sesuatu paket data ke PC 172.24.12.18 , maka PC tersebut akan mengecek ARP Cache Table, jika tidak ada dalam table akan melakukan broadcast. Lalu PC yang dituju akan memberikan respon berupa *MAC Address*, selanjutnya disimpan di PC yang meminta. (Deris Setiawan, 2001).

2.7 Wireless Access Point

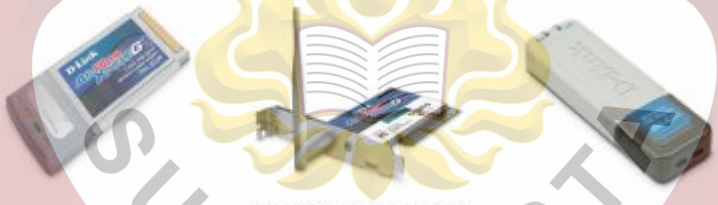
Wireless Access Point merupakan suatu perangkat yang digunakan untuk menghubungkan pengguna dengan jaringan komputer biasa. Access Point ini menerima data dari pengguna dalam bentuk gelombang frekuensi radio dan kemudian meneruskannya ke jaringan kabel, sebaliknya *access point* juga mengirimkan data dari jaringan ke pengguna dalam bentuk gelombang radio. (www.if.lib.itb.ac.id, 2005).

Gambar 2.1 Wireless Access Point

Dalam satu lingkup jaringan komputer dapat terdiri dari satu atau beberapa *access point* yang mengidentifikasikan suatu jaringan tersebut. Karena *access point* merupakan gerbang bebas yang berhubungan langsung dengan pengguna, maka *access point* ini juga dilengkapi berbagai teknik keamanan agar koneksi dari pengguna .

2.8 Wireless Adapter

WLAN terdiri dari dua komponen utama, yaitu *access point* yang akan melakukan koneksi ke jaringan, dan *adapter wireless* yang terkoneksi pada peralatan komputer *client*. Adapter wireless mempunyai fungsi yang sama seperti dengan NIC pada jaringan wired tradisional. Ada beberapa bentuk adapter wireless diantaranya seperti : Wireless Card PCI Adapter, USB wireless adapter dan PCMCIA. (Departemen Teknik Informatika ITB, 2005).



Gb 5: Perangkat client

Gambar 2.2 Wireless Adapter Client

2.9 Wireless Access Point Security

Daerah diantara *access point* dengan pengguna merupakan daerah dengan kemungkinan gangguan keamanan paling tinggi dari jaringan nirkabel. Daerah ini merupakan daerah bebas, dimana komunikasi data dilakukan melalui frekuensi radio sehingga berbagi gangguan keamanan dapat terjadi di sini. Secara umum gangguan keamanan yang ada di daerah antara *access point* dengan pengguna adalah: autentifikasi dan *eavesdropping* (penyadapan). *Access point* harus bisa menentukan apakah seorang pengguna yang berusaha membangun koneksi ke jaringan tersebut

memiliki hak akses atau tidak dan juga berusaha agar komunikasi dengan pengguna dilakukan secara aman.

Selama ini ada beberapa teknik yang digunakan untuk mendukung keamanan *Access Point*, diantaranya:

2.9.1 Service Set ID

Service Set ID atau SSID merupakan 32 karakter unik yang mengidentifikasikan suatu jaringan nirkabel. Jika dalam satu jaringan terdapat beberapa *access point*, maka *access point* tersebut mengidentifikasikan satu jaringan yang sama, dengan kata lain *access point* tersebut memiliki SSID yang sama. Pengguna harus mengetahui SSID *Access Point* yang bersangkutan jika ingin melakukan koneksi.

Jika kita membeli *Access Point*, secara *default Access Point* tersebut telah dikonfigurasikan oleh vendor pembuatnya. Konfigurasi awal ini memungkinkan *access point* untuk menyebarkan (*broadcast*) SSID setiap selang waktu tertentu. *Broadcast* SSID ini memungkinkan setiap pengguna yang berada dalam cakupan *access point* dapat mengetahui SSID jaringan tersebut sehingga pengguna yang sebenarnya tidak berhak mengakses, dapat mengakses jaringan tersebut. Hal ini merupakan kelemahan tersendiri bagi *access point*. Untuk mengatasi kelemahan tersebut, sebaiknya konfigurasi awal dari vendor pembuatnya diubah, terutama menonaktifkan *broadcast* SSID sehingga pengguna harus mengetahui SSID dari *access point* jika ingin melakukan koneksi ke jaringan yang bersangkutan.

2.9.2 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) dinamakan demikian dengan maksud agar WEP memiliki tingkat keamanan yang setara dengan jaringan *wired* (jaringan kabel). Seperti kita ketahui jaringan kabel memiliki tingkat keamanan yang cukup baik dan lebih baik jika dibandingkan dengan jaringan nirkabel. WEP digunakan untuk keamanan transfer data melalui metode enkripsi dan dekripsi, selain

itu WEP dapat juga digunakan untuk autentifikasi pengguna melalui protokol WEP. WEP menggunakan algoritma RC4 yang merupakan algoritma kriptografi *stream chipper*. Pesan di enkripsi terlebih dahulu sebelum dikirimkan dan sebuah *Integrity check* akan memeriksa apakah terjadi perubahan pada pesan yang dikirimkan. Untuk melakukan enkripsi suatu pesan atau data digunakan kunci rahasia dan *initial vector* (IV). Panjang kunci ini antara 64 bit sampai 128 bit, sedangkan IV merupakan nilai random atau juga bisa masukan pengguna yang panjangnya 24 bit.

Metode WEP ini setidaknya memiliki dua kelemahan, yaitu dalam hal manajemen kunci dan *chipertext attack*. Seperti yang sudah dijelaskan di atas, pada umumnya, WEP menerapkan manajemen kunci yang statis. Satu kunci untuk semua pengguna dan berlaku selamanya. Hal ini menyebabkan jika ada pengguna yang sebenarnya tidak memiliki hak akses dapat mengetahui kunci (*shared key*), maka ia dapat melakukan koneksi ke jaringan dengan bebas dan gratis selama kunci tersebut berlaku. WEP juga rentan dengan serangan *chipertext attack*. Jika seorang penyadap dapat memperoleh dua *chipertext* yang dikirimkan menggunakan algoritma RC4, misalnya c1 dan c2, maka ia bisa memperoleh kunci (*shared key*) yang digunakan untuk mendeskripsikan *chipertext* tersebut. (Edi S Mulyanta , 2005).

2.9.3 MAC Address Filtering

Media Access Control Address adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis *Ethernet, MAC Address* merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan.

MAC Address juga sering disebut sebagai *Ethernet address, physical address*, atau *hardware address.* Dalam sebuah komputer, *MAC Address* ditetapkan ke sebuah kartu jaringan (*network interface card/NIC)* yang digunakan untuk menghubungkan komputer yang bersangkutan ke jaringan. *MAC Address* umumnya tidak dapat diubah karena telah dimasukkan ke dalam ROM. Beberapa kartu jaringan menyediakan utilitas yang mengizinkan pengguna untuk mengubah *MAC Address*, meski hal ini kurang disarankan. Jika dalam sebuah jaringan terdapat dua kartu jaringan yang memiliki *MAC Address* yang sama, maka akan terjadi konflik alamat dan komputer pun tidak dapat saling berkomunikasi antara satu dengan lainnya. Beberapa kartu jaringan, seperti halnya kartu *Token Ring* mengharuskan pengguna untuk mengatur *MAC Address* (tidak dimasukkan ke dalam ROM), sebelum dapat digunakan.

MAC Address memang harus unik, dan untuk itulah *Institute of Electrical and Electronics Engineers (IEEE)* mengalokasikan blok-blok dalam *MAC Address*. 24 bit pertama dari *MAC Address* merepresentasikan siapa pembuat kartu tersebut, dan 24 bit sisanya merepresentasikan nomor kartu tersebut. Setiap kelompok 24 bit tersebut dapat direpresentasikan dengan menggunakan enam digit bilangan heksadesimal, sehingga menjadikan total 12 digit bilangan heksadesimal yang merepresentasikan keseluruhan *MAC Address*.

Daftar pengguna yang berhak mengakses jaringan disimpan di dalam *Access Control List* (ACL). Jika ada pengguna yang berusaha untuk membangun koneksi dengan jaringan maka *access point* akan memeriksa *MAC Address* dari pengguna, kemudian memeriksa apakah *MAC Address* tersebut ada di dalam ACL atau tidak, jika ada maka pengguna tersebut boleh mengakses jaringan dan jika tidak maka permintaan koneksinya ditolak. Berikut merupakan tabel beberapa pembuat kartu jaringan populer dan nomor identifikasi dalam *MAC Address:*

Tabel 2.2 Nomor identifikasi dalam MAC Address

Nama vendor	**Alamat MAC**
Cisco System	00 00 0C
Cabletron System	00 00 1D
International Business Machine Corporation	00 04 AC
3Com Corporation	00 20 AF
GVC Corporation	00 C0 A8
Apple Computer	08 00 07
Hewlett-Packard Company	08 00 07

2.10 Prinsip Penyaluran Sinyal

Transmisi pada *Local Area Network* dapat dibagi ke dalam tiga kategori utama, yaitu: *unicast, multicast dan broadcast* yang masing-masing akan kita bahas berikut ini:

2.10.1 Unicast

Unicast merupakan transmisi jaringan *one to one*. Ketika digunakan, satu sistem tunggal hanya mencoba berkomunikasi dengan satu sistem lainnya. Pada jaringan *Ethernet*, penggunaan *unicast* dapat diketahui dengan melihat *MAC address* asal dan tujuan yang merupakan alamat host yang unik. Pada jaringan yang menggunakan IP, alamat IP asal dan tujuan merupakan alamat yang unik.

Ketika sistem berhubungan dengan frame jaringan, ia akan selalu memeriksa *MAC address* miliknya untuk melihat apakah frame tersebut ditujukan untuk dirinya, jika MAC address-nya cocok dengan sistem tujuan, ia akan memprosesnya. Jika tidak, frame tersebut akan diabaikan. Ingat, ketika dihubungkan ke hub, semua sistem melihat semua frame yang melalui jaringan, karena mereka semua bagian dari *collision domain* yang sama.

2.10.2 Multicast

Multicast merupakan transmisi yang dimaksudkan untuk banyak tujuan, tetapi tidak harus semua host. Oleh karena itu, multicast dikenal sebagai metode transmisi *one to many* (satu ke banyak). Multicast digunakan dalam kasus-kasus tertentu, misalnya ketika sekelompok komputer perlu menerima transmisi tertentu.

Salah satu contohnya adalah *streaming audio* atau video. Misalkan banyak komputer ingin menerima transmisi video pada waktu yang bersamaan. Jika data tersebut dikirimkan ke setiap komputer secara individu, maka diperlukan beberapa aliran data. Jika data tersebut dikirimkan sebagai *broadcast*, maka tidak perlu lagi proses untuk semua system. Dengan *multicast* data tersebut hanya dikirim sekali, tetapi diterima oleh banyak sistem.

Protokol-protokol tertentu menggunakan range alamat khusus untuk *multicast*. Sebagai contoh, alamat IP dalam kelas D telah direservasi untuk keperluan *multicast*. Jika semua host perlu menerima data video, mereka akan menggunakan alamat ip *multicas*t yang sama. Ketika mereka menerima paket yang ditujukan ke alamat tersebut, mereka akan memprosesnya. Ingatlah bahwa system masih tetapi memiliki alamat IP mereka sendiri-mereka juga mendengarkan alamat *multicast* mereka.

2.10.3 Broadcast

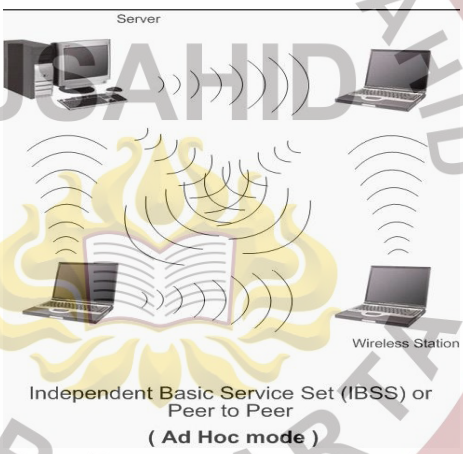
Jenis transmisi jaringan yang terakhir adalah *broadcast*, yang juga dikenal sebagai metode transmisi *one to all* (satu ke semua). Walaupun *broadcast* cenderung membuang resource, beberapa protokol seperti ARP, bergantung kepadanya. Dengan demikian, terjadinya beberapa traffic broadcast tidak dapat dihindari. Pada jaringan *ethernet*, *broadcast* dikirim ke alamat tujuan broadcast dikirim ke alamat tujuan khusus, yaitu, FF-FF-FF-FF-FF-FF-FF-FF. *Broadcast* ini harus diproses oleh semua host yang berada dalam *broadcast domain* yang ditentukan.

2.11 Topologi Jaringan Wireless

Mode topologi jaringan wireless yang dikenal dalam standar 802.11 adalah:

2.11.1 Independent Basic Service Set (IBSS)

Topologi ini dikenal sebagai jaringan *Ad-Hoc*, adalah topologi dimana node-node yang independen akan saling berkomunikasi secara *peer to peer* atau *point to point*. Standar ini merujuk pada topologi *Independent Basic Service Set (IBSS)* dimana salah satu node akan ditunjuk sebagai *proxy* untuk melakukan koordinasi antar mode dalam sebuah grup.



Gambar 2.3 Komunikasi peer to peer pada jaringan Ad-Hoc

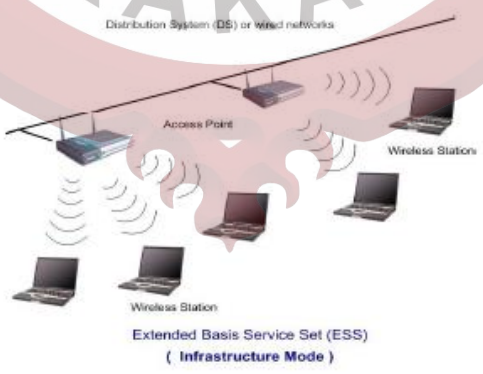
2.11.2 Basic Service Set (BSS)

Topologi ini dikenal sebagai jaringan *Infrastructure*, dimana 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.

Gambar 2.4 Topologi Basic Service Set (BSS)

2.11.3 Extended Service Set (ESS)

Pada topologi ini beberapa access point dapat digunakan untuk mengcover range area yang lebih luas, sehingga membentuk *Extended Service Set* (ESS). Metode ini terdiri dari dua atau lebih BSS 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 seluler. User dapat melakukan roaming ke sel lain dengan cukup mudah tanpa kehilangan sinyal.



Gambar 2.5 Extended Service Set (ESS)

2.12 Model Open System Interconnection (OSI)

Model OSI adalah suatu dekripsi abstrak mengenai desain lapisan-lapisan komunikasi dan protokol jaringan komputer yang dikembangkan sebagai bagian dari inisiatif Open Systems Interconnection (OSI). Model ini disebut juga dengan model tujuh lapisan OSI (*OSI seven layer model*). Model arsitektural yang dikembangkan oleh badan *International Organization for Standardization* (ISO) di Eropa pada tahun 1974. OSI sendiri merupakan singkatan dari *Open System Interconnection*. (www.id.wikipedia.org, 2007).

Tabel 2.3 Model *Open System Interconnection* (OSI)

Lapisan ke-	**Nama lapisan**	**Keterangan**
7	*Application layer*	Berfungsi sebagai antar muka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.
6	*Presentation layer*	Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga Network shell (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol*
5	*Session layer*	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

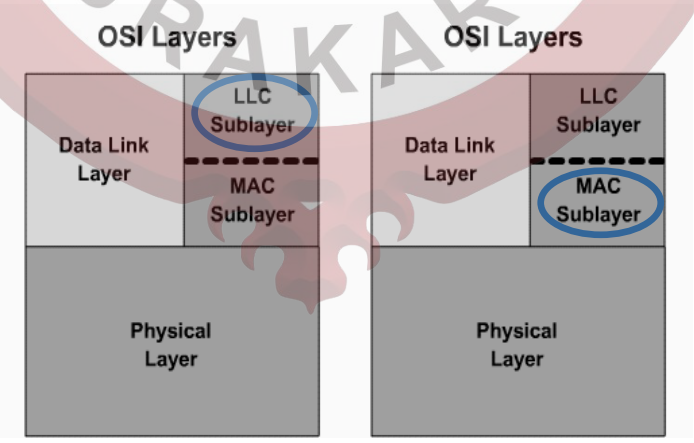
4	*Transport layer*	Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.
3	*Network layer*	Berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan routing melalui *internetworking* dengan menggunakan router dan switch layer-3.
2	*Data-link layer*	Berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch* layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).
1	*Physical layer*	Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengkabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

2.13 Memahami Data Link Layer

Layer data link melakukan manajemen pengalamatan secara fisik dalam *MAC address* dan mengatur akses pada peralatan jaringan dalam media physical. Berdasarkan kompleksitas tugasnya, layer data link dibagi menjadi dua sub layer, yaitu *Logical Link Control* (LLC) dan *media access control* (MAC)

Sub layer LLC terdiri dari data link layer pada setengah bagian atasnya, yang berfungsi sebagai interface layer di atasnya, yaitu layer network dan interface bagian sub layer dibawahnya, yaitu MAC. Sub layer LLC akan melakukan enkapsulasi dari layer 3 dengan menambahkan angka urutan dan penanda. Sub layer LLC menyediakan layanan yang berlainan tergantung software jaringannya.

Sub layer *logical link control* (LLC) akan mengatur komunikasi diantara peralatan-peralatan melalui link tunggal jaringan, sedangkan *media access control* (MAC) merupakan sub layer yang mengatur akses protokol ke media fisik jaringan. Spesifikasi MAC oleh IEEE berisi alamat MAC, yang dapat digunakan pada beberapa model peralatan. MAC akan memberikan identitas unik yang dapat digunakan pada beberapa peralatan yang telah tersedia.



Gambar 2.6 Sub Layer Pada Data Dink

2.14 Fungsi Layer MAC 802.11

Berikut akan dibahas beberapa fungsi umum pada MAC:

2.14.1 Scanning

Standar 802.11 mempunyai dua metode *scanning*, yaitu metode aktif dan pasif. *Scanning* secara pasif dilakukan oleh setiap NIC secara individual untuk mencari sinyal terbaik di *access point*. Secara periodik, *access point* akan melakukan pemancaran *broadcast* dan NIC radio akan menerima pancaran tersebut saat melakukan scanning serta melakukan pencatatan kekuatan sinyal. Pancaran tersebut berisi informasi tentang *access point* yang meliputi *Service Set Identifier* (SSID), data rate dan lain-lain. NIC radio dapat menggunakan informasi ini selama sinyal tersebut kuat.

Metode *scanning* yang lain adalah metode aktif, dimana NIC radio berinisiatif untuk melakukan broadcast sebuah *frame probe*, dan semua *access point* yang ada di dalam range tersebut akan meresponnya dengan mengirimkan probe respon. *Scanning* aktif akan menjadikan NIC radio selalu menerima dengan segera respon dari *access point* , tanpa menunggu transmisi pemancar.

2.14.2 Autentikasi

Adalah proses pencocokan identitas. Pada standar 802.11 telah ditentukan dua bentuk autentikasi, yaitu *open system authentication* dan *shared authentication.*

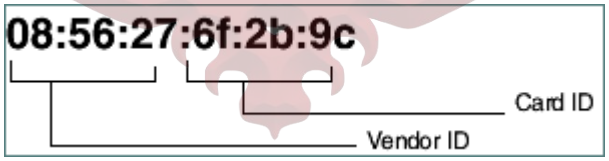
2.14.3 Association

Saat autentikasi, NIC radio harus bergabung 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 merespon dengan mengirimkan *association request 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.

2.15 Pengalamatan Pada MAC

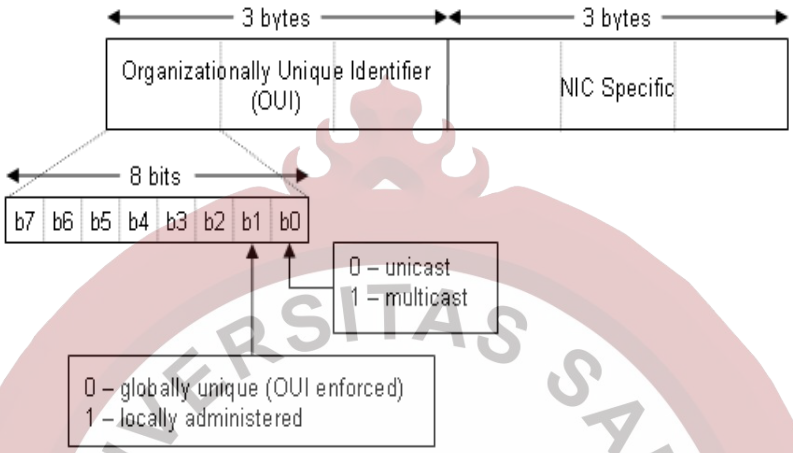
Pengalamatan pada *Media Access Control* (MAC) terdiri dari subset alamat pada link layer. Alamat MAC mengidentifikasi entitas jaringan dalam LAN dengan mengimplementasikan pengalamatan MAC IEEE pada layer data link. Pada pengalamatan data link, alamat MAC merupakan nilai yang unik pada setiap interface LAN. Alamat MAC terdiri dari 48 bit panjangnya dan mempunyai 12 digit hexadecimal. 6 digit hexadecimal pertama digunakan oleh IEEE, yang berisi identitas pabrikan atau vendor dalam satu organisasi *Organizational Unique Identifier* (OUI). 6 digit hexadecimal terakhir terdiri dari nomor serial interface yang digunakan oleh vendor. Alamat MAC ini terkadang diberi nama dengan *burned-id address* (BIA) karena ditempatkan ke dalam *read only memory* (ROM) dan disalinkan di *random access memory* (RAM) saat kartu interface tersebut diinisialisasi. *Hexadecimal* menggunakan digit 0 hingga 9 dan huruf A hingga f, dimana setiap digit akan dipisahkan oleh tanda titik dua, misalnya 08:56:27:6f:2b:9c. (Tutun Juhana, 2003).



Gambar 2.7 Pengalamatan MAC Address

Format pengalamatan *MAC address* sekarang secara resmi disebut dengan MAC-48, nama ini diambil dari spesifikasi *ethernet* yaitu

menggunakan ruang alamat 48 bit. Secara detail pengalamatan *MAC address* dapat ditunjukkan pada gambar 2.8



Gambar 2.8 Alamat detail MAC Address