# BAB III
# STANDAR *IEEE 802.11b*

## 3.1. Sejarah Jaringan Komputer Nirkabel [5]

Pada tahun 1971 untuk pertamakalinya teknologi jaringan komputer digabungkan dengan teknologi komunikasi radio di Universitas Hawai dibawah proyek yang disebut dengan *ALOHANET. ALOHANET* membuat komputer-komputer yang terdapat pada tujuh kampus yang tersebar di empat pulau dapat saling berkomunikasi dengan komputer pusat di Ohau tanpa menggunakan jalur telepon yang mahal dan tidak stabil. *ALOHANET* menawarkan komunikasi dua arah dalam bentuk jaringan bintang (*star topology*) antara komputer utama dan komputer-komputer *remote* lainnya, sehingga untuk saling berkomunikasi komputer-komputer *remote* harus melalui komputer sentral terlebih dahulu.

Pada tahun 1980 seorang penggemar radio amatir yang bernama *Hams* membuat hubungan jaringan komputer radio antara Amerika Serikat dan Kanada dengan mendesain dan membuat *Terminal Node Controllers (TNCs)* yang menjadi antarmuka antara komputer dengan peralatan radio milik *Hams*. *Terminal Node Controllers* berfungsi lebih sebagai *modem* telepon, yang mengubah sinyal digital menjadi sinyal yang dapat dimodulasi dan dikirimkan melalui gelombang radio dengan menggunakan teknik *paket switching*. Ini yang kemudian mendorong *American Radio Relay League (ARRL)* dan *Canadian Radio Relay League (CRRL)* untuk mensponsori konferensi jaringan komputer/*Computer Networking Conference* diawal dekade 80an untuk menyediakan forum bagi pengembangan *Wireless Wide Area Network (WAN)*. Meskipun demikian *Hams* telah menggunakan jaringan komputer nirkabel selama bertahun-tahun dan jauh lebih awal daripada pasar komersial.

Pada tahun 1985 *Federal Communications Commission (FCC)* menetapkan penggunaan frekuensi antara 902 Mhz hingga 5.85 Ghz yang berada diatas frekuensi operasi telepon selular sebagai pita *Industry, Scientific, and Medical (ISM)* yang menyebabkan pesatnya pengembangan secara komersial peralatan jaringan komputer yang berbasiskan radio. Pita gelombang *ISM* sangat menarik bagi *vendor-vendor* jaringan komputer nirkabel karena pita gelombang ini menyediakan tempat untuk beroperasi bagi produk-produk mereka, dan pengguna akhir tidak harus memiliki lisensi *FCC* untuk menjalankan peralatan *Wireless LAN*.

Alokasi pita gelombang *ISM* memiliki dampak yang dramatis sekali terhadap teknologi nirkabel dan mempercepat pengembangan peralatan *Wireless LAN*, meskipun begitu dengan tidak adanya standar membuat *vendor-vendor* mengembangkan peralatan radio dan *access point* versi mereka sendiri.

Di akhir dekade 80an grup kerja *Institute for Electrical and Electronic Engineers (IEEE) 802* yang bertanggung jawab untuk pengembangan standar *Local Area Network (LAN)* seperti *ethernet* dan *token ring* memulai pengembangan untuk standar *Wireless LAN*. Dibawah pimpinan Vic Hayes, seorang teknisi dari *NCR*, grup kerja yang dinamai *IEEE 802.11* ini mengembangkan spesifikasi *Medium Access Control (MAC)* dan *Physical Layer (PHY)* dari *Wireless LAN.*

Dewan standar *IEEE* menyetujui standar baru ini pada tanggal 26 Juni 1997, dan *IEEE* mempublikasikan standar *802.11* pada tanggal 18 November 1997. Penyelesaian standar ini menyebabkan *vendor* harus membuat kartu *adapter Wireless LAN* dan *access point* yang sesuai dengan standar *802.11* pada tahun 1998, *vendor* baru lainnya yang baru memasuki pasar dipastikan juga akan mengembangkan dan merilis produk yang menggunakan standar yang disetujui oleh kelompok kerja *IEEE 802.11*.

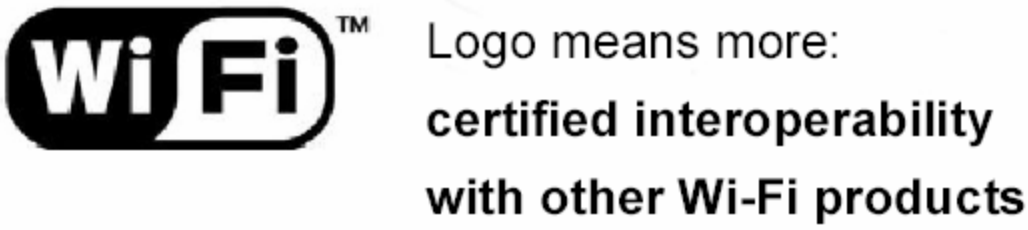
Generasi pertama dari spesifikasi ini hanya memiliki kemampuan mentransfer data sebesar 1 Mbps dan 2 Mbps.

Melihat masa depan teknologi ini yang cerah, komite ini memperkirakan beberapa tahun ke depan dunia akan membutuhkan lebar pita yang lebih besar karena itu teknologi yang lebih maju dan cepat akan dibutuhkan, segera komite ini bekerja lagi untuk mengembangkan standar *802.11* yang dapat memenuhi tuntutan masa depan. Pada bulan September 1999, kelompok kerja ini menyetujui dua *Project Authorization Request (PAR)* untuk pengembangan standar *802.11 physical layer* yang lebih cepat.

Kedua jenis standar baru ini didesain untuk dapat bekerja pada *layer MAC (Medium Access Control) 802.11* yang telah ada, yang pertama adalah standar *802.11a* yang bekerja pada 5 GHz *Unlicensed National Information Infrastructure (UNII)* dan dapat mentransfer data hingga *54* Mbps, yang kedua adalah standar *802.11b* yang bekerja pada 2.4 GHz dan dapat mentransfer data hingga 11 Mbps.

Meskipun dengan disahkannya standar *IEEE 802.11* ini, namun masih banyak ditemui produk dari berbagai *vendor* yang tidak dapat saling berkomunikasi, ini disebabkan oleh adanya perbedaan-perbedaan dalam mengimplementasikan standar *802.11*. Karena itu pada tahun 1999 dibentuk organisasi yang disebut dengan *Wireless Ethernet Compatibility Alliance (WECA)*. *WECA* merupakan lembaga independen yang bertujuan untuk memastikan bahwa berbagai produk hasil implementasi standar ini dapat saling bekerja sama. Ini dilakukan dengan jalan mengadakan program tes *interoperability* pada setiap produk dari *vendor*, apabila ada produk yang tidak sesuai dengan standar maka *vendor* akan diberitahu untuk memperbaikinya, dan bila telah lulus tes maka produk akan memperoleh sertifikasi *Wi-Fi*™ dan diperbolehkan menyandang logo *Wi-Fi*™ yang diperlihatkan pada Gambar 3.1. pada produknya, dengan adanya logo ini membuat

konsumen tidak perlu khawatir produk yang mereka beli dari merk yang berlainan tidak dapat bekerja sama.




Gambar 3.1. Logo *Wi-Fi*™

Skripsi ini akan memfokuskan pada standar *802.11b* yang saat ini telah banyak tersedia secara komersial produknya, meskipun para *vendor* sendiri sudah mulai merilis produk yang berdasarkan atas standar *802.11a*.

### 3.2. Pita frekuensi 2.4 GHz *ISM*

Frekuensi 2.4 GHz dapat digolongkan sebagai gelombang mikro (*Microwave)* yang memiliki karakteristik merambat sejajar garis lurus sehingga kualitas transmisi yang terbaik akan diperoleh apabila kedua piranti yang menggunakan frekuensi ini berada pada jangkauan jarak pandang (*line of sight*) dan tidak terdapat halangan diantaranya, meskipun begitu sebenarnya gelombang 2.4 GHz juga relatif dapat memantul dan menembus benda-benda yang tidak solid, namun ini dipengaruhi oleh banyak faktor antara lain kualitas medium (interferensi, propagasi sinyal, derau/*noise*), tenaga atau daya yang digunakan oleh peranti, dan medium penghalangnya sendiri.

Pita frekuensi 2.4 GHz merupakan pita frekuensi yang dibebaskan lisensi penggunaannya untuk pemakaian pribadi. Meskipun begitu peralatan yang bekerja pada frekuensi ini tetap harus mengikuti peraturan mengenai konsumsi tenaga yang diperbolehkan, karena pada kondisi dunia nyata penggunaan frekuensi dan daya yang tidak terkontrol dapat menyebabkan

interferensi dan berpotensi untuk menurunkan kualitas transmisi.

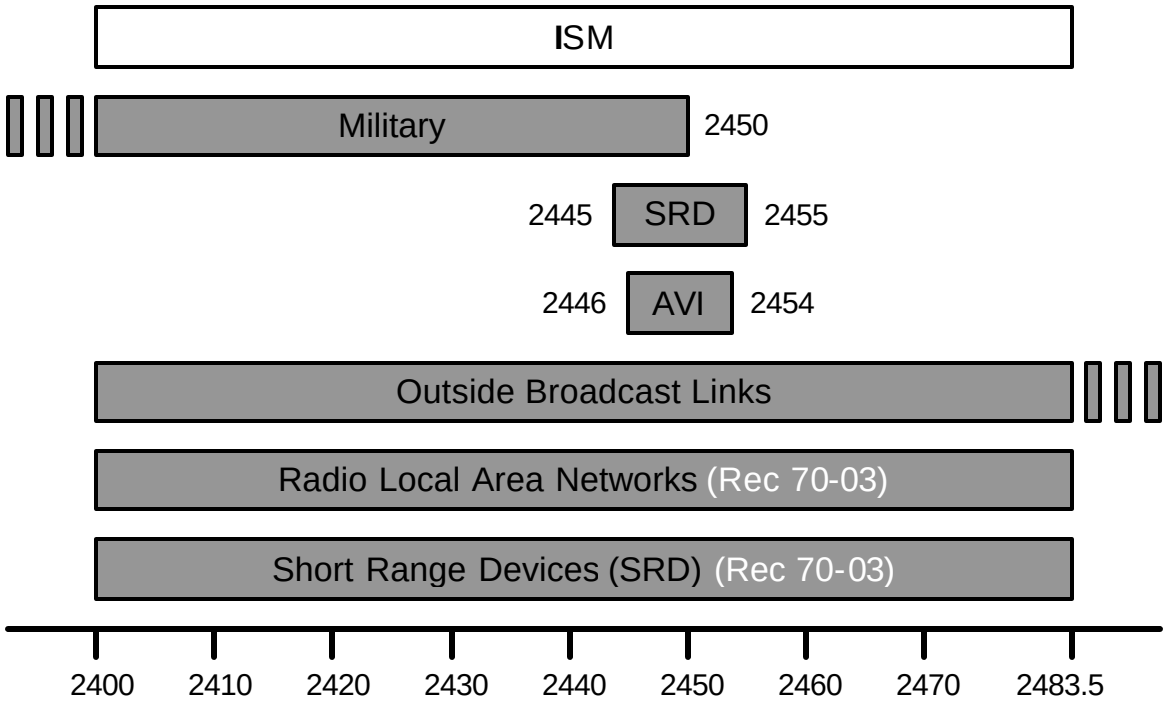
Frekuensi 2.4 GHz ini memiliki beberapa keuntungan. Pertama, frekuensinya yang relatif masih dapat digolongkan sebagai frekuensi rendah membuatnya sangat sesuai untuk komunikasi bergerak. Kedua, tersedianya pita frekuensi ini di seluruh dunia menawarkan kesempatan luas bagi pembuat piranti untuk menekan biaya produksi serta kemudahan beroperasi dan dipasarkan di seluruh dunia.

Berdasarkan sifat alami aplikasi pengguna frekuensi ini dan karakteristik teknik penggunaan spektrum yang ada maka pengguna pita frekuensi ini dapat digolongkan menjadi enam kelompok utama yang tampak pada tabel 3.1., dimana hanya tiga diantaranya yang membayar lisensi penggunaan frekuensi ini.

Tabel 3.1. Kategori pengguna pita frekuensi 2.4 GHz

| Tipe Pengguna | Lisensi frekuensi |
|---|---|
| Militer | Membayar |
| Pengumpulan berita elektronis dan penyebaran informasi televisi | Membayar |
| Pengunaan umum untuk akses nirkabel tetap (*Fixed Wireless Access*) | Membayar |
| Jaringan Nirkabel : | |
| Radio LANs | Dibebaskan |
| *Bluetooth*™ | Dibebaskan |
| *SOHO* dan jaringan rumah | Dibebaskan |
| Peralatan jangkah pendek lainnya : | |
| Peralatan identifikasi *RF* | Dibebaskan |
| Aplikasi Video/*Closed Circuit Television (CCTV)* | Dibebaskan |
| Aplikasi *ISM* : | |
| Oven microwave | Dibebaskan |
| Penyinaran plasma sulfur | Dibebaskan |

Sedangkan gambaran penggunaan pita frekuensi 2.4 GHz ini tampak pada Gambar 3.2. dibawah ini.




Gambar 3.2. Gambaran penggunaan pita frekuensi 2.4 GHz

### 3.3. Berbagai Tipe Standar *802.11* [6]

Hingga saat ini standar *802.11* masih terus dikembangkan oleh *IEEE*, mereka membentuk kelompok-kelompok kerja yang masing-masing memiliki tujuan tersendiri dalam mengembangkan berbagai aspek dari teknologi ini, grup-grup ini dinamai berdasarkan dengan abjad yang ada dibelakang, contohnya *802.11x*. Berbagai jenis standar *802.11* ini:

1. *802.11* (Tahun 1997)

   Standar ini merupakan generasi pertama dari teknologi *Wireless LAN* yang bertujuan untuk mengembangkan spesifikasi *Medium Access Control (MAC)* dan *Physical Layer (PHY)* untuk hubungan nirkabel bagi terminal tetap, portabel, dan bergerak dalam lokal area.

Bekerja pada frekuensi 2.4 GHz, menspesifikasikan tiga macam *physical layer* yaitu:

1. *Frequency Hopping Spread Spectrum (FHSS)*
2. *Direct Sequence Spread Spectrum (DSSS)*
3. Infra Merah/*Infra Red (IR)*

*802.11* memiliki dua kecepatan transmisi yaitu:

a. 1 Mbps, menggunakan modulasi *Differential Binary Phase Shift Keying (DBPSK).*
b. 2 Mbps, menggunakan modulasi *Differential Quadrature Phase Shift Keying (DQPSK).*

2. *802.11a* (Tahun 1999)

Standar ini mengunakan pita frekuensi baru untuk jaringan *Wireless LAN* dengan peningkatan kecepatan transfer data hingga 54 Mbps dengan digunakannya teknik modulasi *Orthogonal Frequency Division Multiplexing (OFDM).* Standar *802.11a* ini menggunakan pita gelombang *Unlicensed National Information Infrastructure (UNII)* yang mulai banyak digunakan di berbagai bidang teknologi nirkabel, pita ini dibagi menjadi tiga bagian yang berbeda yaitu:

1. *UNII-1* dengan frekuensi pada 5.2 GHz.
2. *UNII-2* dengan frekuensi pada 5.7 GHz.
3. *UNII-3* dengan frekuensi pada 5.8 GHz.

*802.11a* sering dianggap sebagai pendahulu *802.11b*, ini merupakan salah pengertian karena sebenarnya *802.11b* merupakan generasi kedua dan *802.11a* merupakan generasi ketiga, *802.11a* sendiri masih menggunakan *MAC* yang sama seperti pada *802.11* maupun *802.11b* sedangkan perbedaan hanya terdapat pada *physical layer*-nya saja.

3. *802.11b* (Tahun 1999)

   Standar ini masih bekerja pada frekuensi 2.4 GHz seperti *802.11* namun memberikan peningkatan kecepatan transfer 5.5 Mbps dan 11 Mbps, ini dimungkinkan dengan penggunaan teknik modulasi *Complementary Code Keying (CCK)*, standar ini hanya menspesifikasikan penggunaan *DSSS* saja, karena *FHSS* dan infra merah tidak mampu memenuhi tuntutan kecepatan untuk masa depan.

   Standar ini disebut juga *802.11 High Rate (HR).*

4. *802.11c* (Tahun 1998)

   Grup kerja ini menambahkan dukungan terhadap layanan *sublayer* internal (*Internal Sublayer Service*) pada prosedur *MAC* untuk dapat menjembatani operasi antar *MAC-MAC 802.11*.

5. *802.11d* (Tahun 2001)

   Penambahan grup ini akan bertujuan untuk mendefinisikan kebutuhan *layer physical* seperti pengaturan kanal, pola loncatan sinyal, pemberian atribut pada *MIB (Management Information Base),* dan berbagai kebutuhan lainnya untuk menyesuaikan operasi *Wireless LAN* pada negara-negara yang berbeda.

6. *802.11e*

   Grup kerja ini bertugas meningkatkan kualitas *802.11* (baik *a*, *b*, maupun *g*) agar menyamai kualitas layanan dari *ethernet*, menambahkan *Class of Service* dan mengefisienkan protokol yang akan mendongkrak kecepatan total dari sistem dalam menangani aplikasi seperti audio, video, multimedia *streaming* melalui jaringan nirkabel.

7. *802.11f*

   Grup kerja ini bekerja untuk menyamakan aturan-aturan yang digunakan untuk *Inter-Access Point Protocol (IAPP)* yaitu agar berbagai *access point* dari *vendor* yang berbeda

dapat bekerja sama pada sistem nirkabel terdistribusi yang mendukung *802.11*, sehingga terminal-terminal yang menggunakan *adapter Wireless LAN* dapat melakukan *roaming* antar *access point*.

8. *802.11g*

   Standar *802.11g* atau yang juga disebut dengan *802.11b extended* meningkatkan kecepatan transfer data hingga 54 Mbps pada pita gelombang 2.4 GHz. Pada awalnya terdapat perbedaan pendapat tentang teknik modulasi yang akan digunakan oleh standar ini, namun akhirnya diputuskan penggunaan teknik modulasi *Orthogonal Frequency Division Multiplexing (OFDM)* dengan alternatif penggunaan modulasi *Packet Binary Convolution Coding (PBCC).*

9. *802.11h*

   Grup kerja ini mengembangkan standar untuk penggunaan tenaga baterai dan daya transmisi sinyal radio, juga pemilihan kanal komunikasi yang dinamis. Dibentuknya kelompok kerja ini disebabkan oleh kebutuhan umur pemakaian baterai yang lebih lama dan adanya peraturan *Equivalent Isotropically Radiated Power (EIRP)* di setiap negara.

10. *802.11i*

    Kelompok kerja ini difokuskan untuk mengembangkan protokol keamanan data dan otentikasi pengguna dari seluruh standar *802.11*. Standar keamanan *802.11b* adalah *Wired Equivalent Privacy (WEP)* yang merupakan teknik enkripsi data menggunakan algoritma *RC4* dengan panjang kunci 64 atau 128 bit. Algoritma ini telah diketahui memiliki kelemahan yang memungkinkan jaringan untuk disadap dan diserang.

11. *802.11*j

Kelompok kerja ini menstandarisasi penggunaan frekuensi 5 GHz untuk berbagai teknologi jaringan nirkabel seperti *IEEE, ETSI Hyperlan2, ARIB, HiSWANa.*

Dari berbagai jenis pengembangan standar *IEEE 802.11* yang ada diatas, terdapat empat standar utama yang lebih atau akan populer yaitu *802.11, 802.11b, 802.11a*, dan *802.11g*.

Dibawah diberikan Tabel 3.2. yang dapat menjelaskan perbedaan antara keempat standar yang populer tersebut:

Tabel 3.2. Perbandingan aneka standar *IEEE 802.11*

| Standar | *802.11* | *802.11b* | *802.11*a | *802.11*g |
|---|---|---|---|---|
| Disetujui | Juni 1997 | September 1999 | September 1999 | Mei 2003 |
| Frekuensi Kerja | 2400-2483.5 MHz | 2400-2483.5 MHz | 5150-5250 MHz<br>5250-5350 MHz<br>5725-5825 MHz | 2400-2483.5 MHz |
| Lebar Pita | 83.5 MHz | 83.5 MHz | 300 MHz | 83.5 MHz |
| Kecepatan Transfer Data | 1 Mbps (*FHSS*)<br>1 Mbps (*FHSS*)<br>2 Mbps (*DSSS*) | 1 Mbps<br>2 Mbps<br>5.5 Mbps<br>11 Mbps | 6, 9, 12, 18, 24, 36, 48, dan 54 Mbps | 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, dan 54 Mbps |
| Teknik Spektrum Tersebar | *FHSS*<br>*DSSS* | *DSSS* | *OFDM* | *OFDM* |
| Modulasi | *DQPSK* (2 MBPS)<br>*DBPSK* (1 Mbps) | *CCK*, *PBCC* (11&5.5 Mbps)<br>*DQPSK* (2 MBPS)<br>*DBPSK* (1 Mbps) | 64*QAM* (64-level quadrature amplitude modulation) | *CCK*, dan *PBCC* |
| Protokol Akses | *CSMA/CA* | *CSMA/CA* | *CSMA/CA* | *CSMA/CA* |

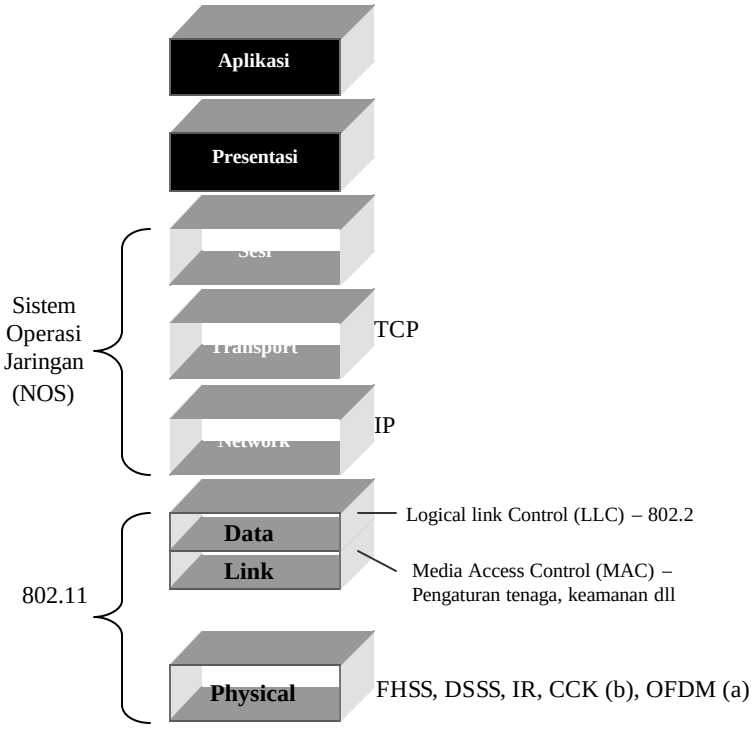
Standar *802.11a* memiliki performa lebih baik dan dapat memenuhi kebutuhan *bandwidth* di masa mendatang, namun *802.11*a juga memiliki beberapa kekurangan bila dibandingkan dengan *802.11b*, karena menggunakan frekuensi yang lebih tinggi membuat jangkauan jaraknya relatif lebih pendek yaitu sekitar

50 meter dibandingkan dengan 100 meter pada *802.11b*, gelombang 5 GHz juga relatif lebih sulit menembus benda-benda padat.

Kekurangan yang lain dari standar *802.11* ini yaitu karena *802.11b* dan *802.11a* menggunakan teknik radio dan modulasi yang berbeda maka keduanya tidak dapat saling berkomunikasi. Karena itu *IEEE* membentuk grup kerja *IEEE 802.11g* yang bekerja untuk meningkatkan kecepatan transfer data pada frekuensi 2.4 GHz hingga 54 Mbps sehingga memiliki transfer data setara dengan *802.11a* namun tidak memiliki kekurangan dalam masalah jarak jangkauan, serta masih kompatibel dengan peralatan yang menggunakan standar *802.11b.*

### 3.4. *Layer-layer 802.11* [11]

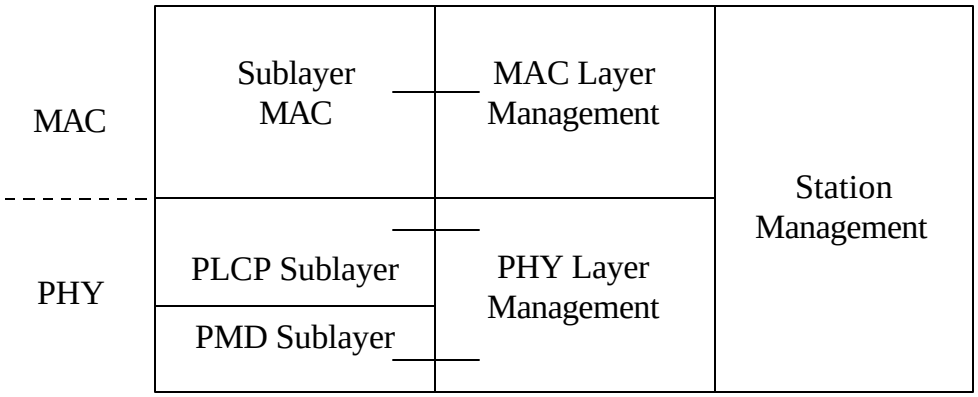
Dari ketujuh *layer* yang dispesifikasikan pada model *ISO OSI*, standar *IEEE 802.11* hanyalah berfungsi sebagai pengganti dari dua lapisan yang paling bawah, yaitu *Data Link Layer* dan *Physical Layer*, sedangkan *layer* sisanya tetap sama.




Gambar 3.3. *Layer-layer 802.11*

Spesifikasi *IEEE 802.11* hanya mendefinisikan *Physical Layer (PHY)* dan *Media Access Control (MAC)* dari model *OSI* seperti yang terlihat pada Gambar 3.3. diatas.

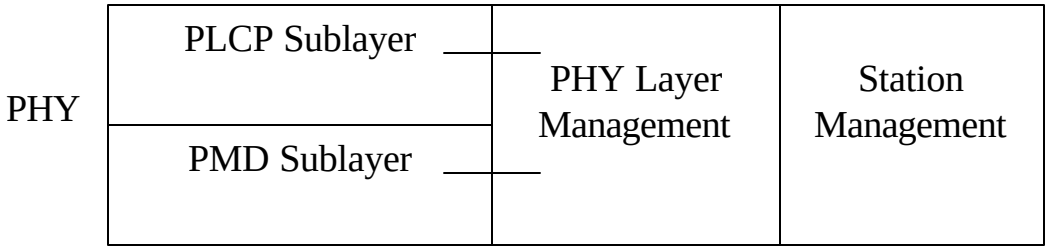
Secara detil *802.11b* memiliki *sublayer-sublayer* yang diperlihatkan pada Gambar 3.4. [7] dibawah ini:




Gambar 3.4. *Sublayer-sublayer 802.11*

### 3.4.1. *Physical Layer (PHY)*

*Physical layer* dari *802.11* merupakan antar muka antara *MAC (Media Access Control)* dengan medium komunikasi dimana *frame-frame* data dikirim dan diterima.




Gambar 3.5. *Sublayer PLCP*

Diperlihatkan pada Gambar 3.5. diatas *PHY* dibagi menjadi tiga bagian *sublayer* [7] yaitu:

a. *Physical Layer Convergence Protocol (PLCP)*, bertugas sebagai antarmuka dengan *MAC*, menyediakan *carrier sense dan Clear Channel Assessment (CCA).*

   *PLCP* beradaptasi dengan kemampuan *Physical Medium Dependent (PMD)* dan layanan *PHY* untuk mengatur bagaimana *MAC sublayer Protocol Data Units (MPDU)* diubah menjadi *frame-frame* data yang dapat dikirim dan diterima.

   *PHY* menggunakan *PHY Protocol Data Units (PPDU)* yang berisi *PLCP Service Data Units (PSDU)*, sedangkan *MAC* sendiri menggunakan layanan *PHY*, jadi setiap *MPDU* berhubungan dengan setiap *PSDU* yang dibawa didalam *PPDU.*

b. *Physical Medium Dependent (PMD),* menyediakan metode untuk mentransmisi dan menerima data melalui medium nirkabel/*Wireless Medium (WM)* antar dua atau lebih terminal, juga bertanggung jawab terhadap pengkodean data, *error* koreksi, modulasi data.

c. *Physical Layer Management Entity (PLME)* dan *Station Management* berfungsi untuk mengatur fungsi *PHY* dalam hubungannya dengan *MAC management entity*.

#### 3.4.1.1. *Physical Layer Convergence Protocol (PLCP)*

*Layer physical* menyediakan teknik yang disebut dengan *Clear Channel Assessment (CCA)* [4] untuk memindai medium untuk mengetahui apakah medium/kanal sedang sibuk (digunakan oleh terminal yang lain), ini dilakukan dengan menggunakan algoritma *CCA* yang memiliki 3 metode pendeteksian medium:

1. *CCA mode 1*, mengukur energi frekuensi radio/aras tenaga di antena dan menentukan kuatnya sinyal yang diterima, sinyal yang telah diukur ini disebut dengan *Received Signal Strength Indication (RSSI),* jika

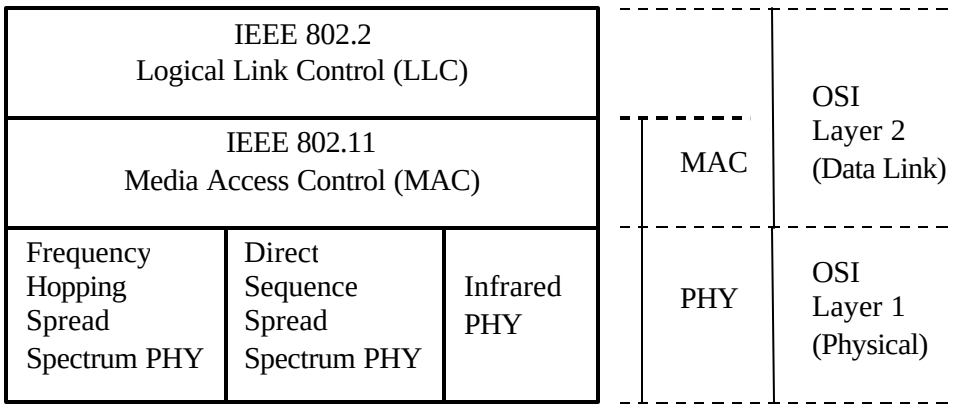
kekuatan sinyal yang diterima berada dibawah ambang batas, maka kanal dikatakan sedang bebas dan *MAC* diberikan status bebas untuk transmisi data.

2. *CCA mode 4*, memindai medium dengan pewaktu, algoritma *CCA* menjalankan pewaktu dengan durasi 3.65 ms dan melaporkan kanal yang sibuk hanya pada saat terdeteksi adanya sinyal pembawa dari *802.11b*, *CCA* akan melaporkan bahwa kanal sedang bebas setelah pewaktu selesai atau tidak ada sinyal pembawa dari *802.11b* yang terdeteksi.
3. *CCA mode 5*, merupakan kombinasi dari memindai medium dengan pewaktu dan pengecekan aras tenaga pada antena, *CCA* akan melaporkan kanal sibuk saat memindai medium dan menemukan adanya sinyal pembawa *802.11b* dan nilai aras tenaga pada antena diatas ambang batas.

Dengan ketiga metode *CCA* diatas diharapkan dapat digunakan untuk mengetahui keadaan kanal dengan sebaik mungkin meskipun juga dipengaruhi oleh tingkat interferensi dan derau/*noise* dari lingkungan sekitarnya.

*Layer Physical 802.11* yang diperlihatkan pada Gambar 3.6. dibawah mendefinisikan tiga alternatif cara penggunaan media transmisi yaitu:

*1.* Infra merah/*Infra Red (IR)*
*2.* Frekuensi loncat spektrum tersebar/*Frequency Hoping Spread Spectrum (FHSS)*
*3.* Frekuensi urut spektrum tersebar/*Direct Sequence Spread Spectrum (DSSS)*




Gambar 3.6. *Physical layer 802.11*

### 3.4.1.2. Infra Merah [8]

*Infra Red physical layer* menggunakan cahaya infra merah untuk mentransmisikan data biner baik pada kecepatan 1 Mbps ataupun 2 Mbps, yang masing-masing menggunakan teknik modulasi sendiri-sendiri, untuk kecepatan 1 Mbps digunakan teknik modulasi 16 posisi pulsa/*16 Pulse Position Modulation (PPM)*, konsep dari *PPM* adalah menvariasikan posisi dari pulsa untuk mewakili simbol biner yang berbeda, sedangkan untuk kecepatan 2 Mbps digunakan teknik modulasi *4 PPM*.

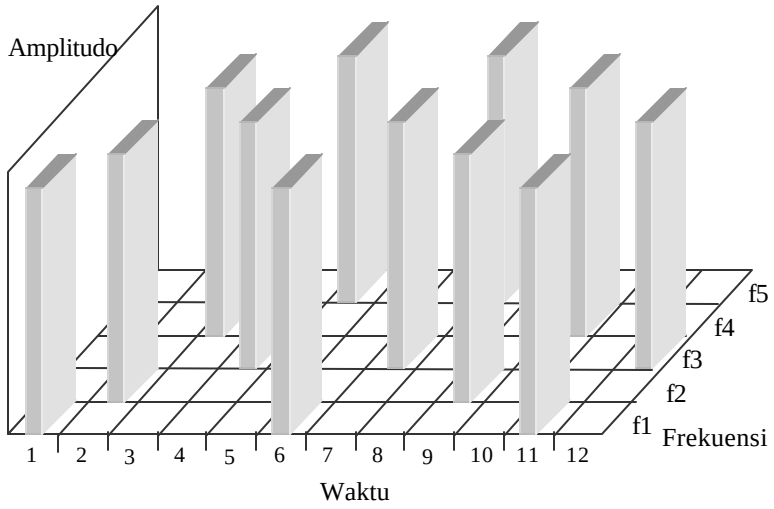
Cahaya yang digunakan beroperasi pada panjang gelombang 850 hingga 950 nano meter dengan tenaga maksimum yang diperbolehkan adalah 2 *Watt*.

Cahaya infra merah tidak dapat menembus benda-benda padat, dan ini merupakan teknologi yang mengharuskan pengirim dan penerima berada di dalam jangkauan jarak pandang (*line of sight*), sistem infra merah yang memiliki daya rendah hanya memiliki jangkauan pendek sekitar satu meter, sedangkan sistem infra merah dengan daya besar tidak praktis untuk pengguna bergerak, karena itu hanya digunakan pada jaringan tetap.

### 3.4.1.3. Frekuensi Loncat Spektrum Tersebar [9]

Frekuensi loncat spektrum tersebar/*Frequency Hopping Spread Spectrum (FHSS)* membawa sinyal data dan memodulasikannya dengan sinyal pembawa yang meloncat dari frekuensi satu ke yang lainnya pada berbagai frekuensi di dalam pita *ISM* sebagai fungsi waktu. Dengan *FHSS* frekuensi pembawa berganti-ganti secara periodik, yang mengurangi interferensi karena sinyal penyebab interferensi hanya akan mempengaruhi sinyal *FHSS* bila memancar pada frekuensi yang sama pada waktu yang sama pula, dengan begitu secara keseluruhan gangguan interferensi akan kecil sekali, sehingga hanya akan ada sedikit atau sama sekali tidak ada kesalahan bit-bit data.

*FHSS* yang diperlihatkan pada Gambar 3.7. dibawah membagi pita 2.4 GHz menjadi kanal-kanal yang masing-masing lebarnya 1 *MHz*, algoritma loncatan yang menggunakan *Pseudorandom Noise Generator (PNG)* akan menentukan pada frekuensi mana dan dengan urutan bagaimana sinyal akan ditransmisikan, untuk dapat menerima sinyal dengan baik penerima harus menyesuaikan dengan algoritma loncatan dan mendengarkan sinyal pada waktu yang tepat dan frekuensi yang tepat. Kecepatan minimum lompatan, jumlah kanal yang digunakan untuk lompatan, dan pembagian kanal ditentukan oleh badan pengatur frekuensi pada masing-masing negara tempat *adapter Wireless LAN* bekerja.




Gambar 3.7. *FHSS*

Jika radio mengalami interferensi pada salah satu frekuensi maka radio akan mengulangi transmisi sinyal yang sama di lompatan yang berikutnya pada frekuensi yang lainnya. Dimungkinkan dua atau lebih radio *FHSS* untuk menggunakan pita gelombang yang sama dan tidak terjadi interferensi, ini dilakukan dengan cara masing-masing radio menggunakan pola lompatan frekuensi yang berbeda-beda.

### 3.4.1.4. Frekuensi Urut Spektrum Tersebar [10]

Dari ketiga media transmisi yang dispesifikasikan pada *IEEE 802.11* yaitu Infra Merah, *FHSS*, dan *DSSS* tersebut kemudian hanya tinggal *DSSS* saja yang masih spesifikasikan pada *IEEE 802.11b* dengan penambahan kecepatan transfer data 5.5 Mbps dan 11 Mbps.

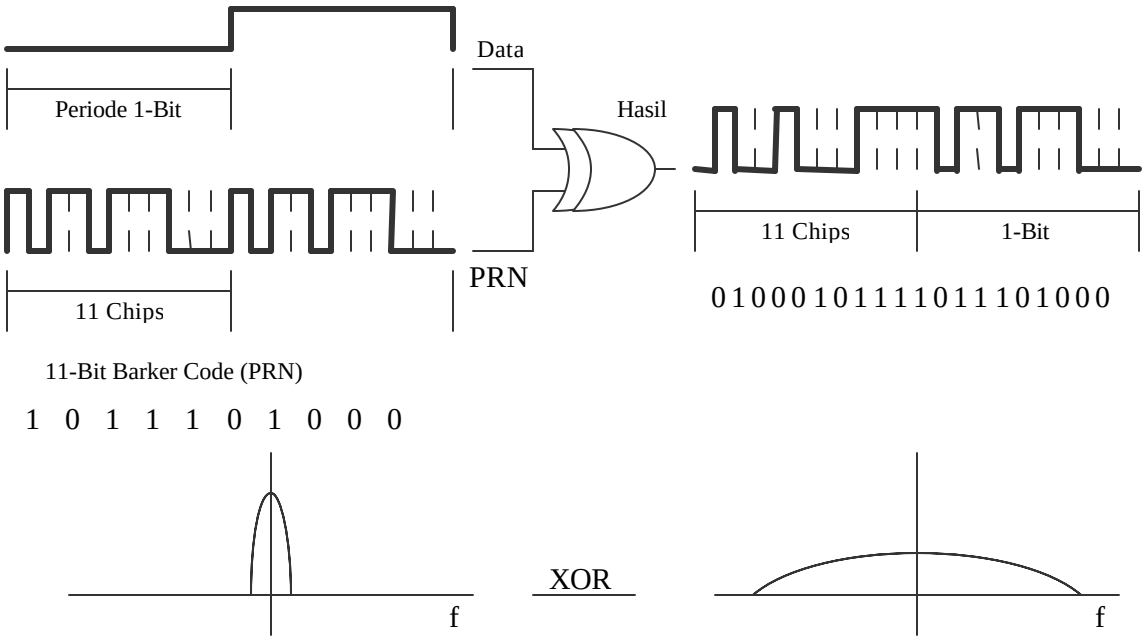
*Direct Sequence Spread Spectrum (DSSS)* yang terlihat pada Gambar 3.8. merupakan teknik penggabungan sinyal data dengan deretan 11 bit yang memiliki kecepatan lebih tinggi yang disebut dengan *11 bit Barker Sequence (chipping code)* untuk mengkodekan data sebelum ditransmisikan, setiap bit dari *barker sequence* disebut dengan *“chip”* untuk membedakan dari

istilah “bit” yang mewakili salah satu informasi biner, setiap bit yang akan ditransmisikan dimodulasikan dengan kesebelas *chip* tersebut dengan jalan meng-*XOR*-kan data dengan *chipping code*.

Meskipun *DSSS* membutuhkan lebar pita yang besar, namun teknik ini lebih kebal terhadap kerusakan data saat transmisi. Ini karena kerusakan pada satu bit data tidak langsung membuat sebuah bit informasi hilang, bahkan pada tingkatan tertentu bila terdapat satu atau lebih bit-bit di dalam *chipping* yang rusak selama transmisi, data yang asli dapat disusun kembali dengan menggunakan teknik statistik tanpa membutuhkan transmisi ulang. Semakin panjang *chipping code* semakin tinggi kemungkinan data yang asli dapat diperoleh tetapi tentu saja dengan membutuhkan lebar pita yang lebih besar.

Hasil dari pengkodean data dengan *chipping code* tersebut adalah aliran data digital yang kemudian dimodulasikan dengan menggunakan metode *PSK*.

Di penerima data diperoleh kembali dengan mengumpulkan semua sinyal spektrum tersebar dan kemudian mendemodulasikannya dengan *chipping code* yang sama pada pengirim.




Gambar 3.8. Penggabungan data *DSSS* dan deretan Barker dengan menggunakan fungsi *XOR*

Bagi pesawat penerima biasa, *DSSS* terlihat seperti derau pita lebar yang memiliki energi rendah dan diblok atau diabaikan oleh kebanyakan penerima pita frekuensi sempit, sering disebut juga dengan *White Noise*. Keuntungan dari teknik ini ialah meminimalisasi efek interferensi dari sumber derau pita sempit.

### 3.4.1.5. Perbandingan antara *FHSS* dan *DSSS*

Dibawah ini diberikan Tabel 3.3. perbandingan antara dua teknik spektrum tersebar, yaitu *FHSS* dan *DSSS*.

Tabel 3.3. Perbandingan *DSSS* dan *FHSS*

| *DSSS* | *FHSS* |
|---|---|
| Memiliki jangkauan lebih jauh | Jangkauan kurang jauh |
| Sulit menginterferensi sistem lainnya | Lebih menginterferensi sistem lainnya |
| *Bandwidth* tergantung pada kecepatan chipping | *Bandwidth* tergantung pada jangkauan radio transmitter |
| Dapat beroperasi dibawah frekuensi *noise* | Harus memiliki nilai *Sinyal to Noise Ratio (SNR)* positif |
| Rentan terhadap masalah degradasi jauh dekat | Lebih kebal terhadap masalah degradasi jauh dekat |
| Menggunakan modulasi koheren yang lebih efisien (menggunakan lebih banyak bit untuk setiap simbol) | Menggunakan modulasi koheren yang kurang efisien |
| Harus menggunakan penguat linier yang lebih mahal | Tidak harus penguat linier, sehingga lebih mudah diimplementasikan |
| Menggunakan *broadband, non-tuneable synthesizer* | Membutuhkan *tuneable synthesizer* |
| Mengatasi interferensi dengan mengurangi terjadinya interferensi | Mengatasi interferensi dengan menghindari interferensi |
| Mengatasi masalah *multipath* dengan mengirim ulang data | Mengatasi masalah *multipath* dengan perpindahan slot frekuensi |

### 3.4.2. *Media Access Control (MAC)*

*Layer MAC* menyediakan fungsi-fungsi yang membuat terjadinya penyampaian data yang stabil ke *layer* yang ada diatasnya dari *layer physical* yang ada dibawahnya, penyampaian data itu sendiri menggunakan metode *asinkron, best effort*, dan *connectionless oriented*.

Selain fungsi utamanya untuk mengatur akses ke medium transmisi yang disebut dengan *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)*, *sublayer MAC* juga memiliki fungsi untuk pengaturan keamanan, fragmentasi paket data dan *Cyclic Redundancy Check (CRC)*.

#### 3.4.2.1. *CSMA/CA* [13]

*MAC* dari *802.11* menyediakan dua metode akses terkontrol ke medium nirkabel yaitu:

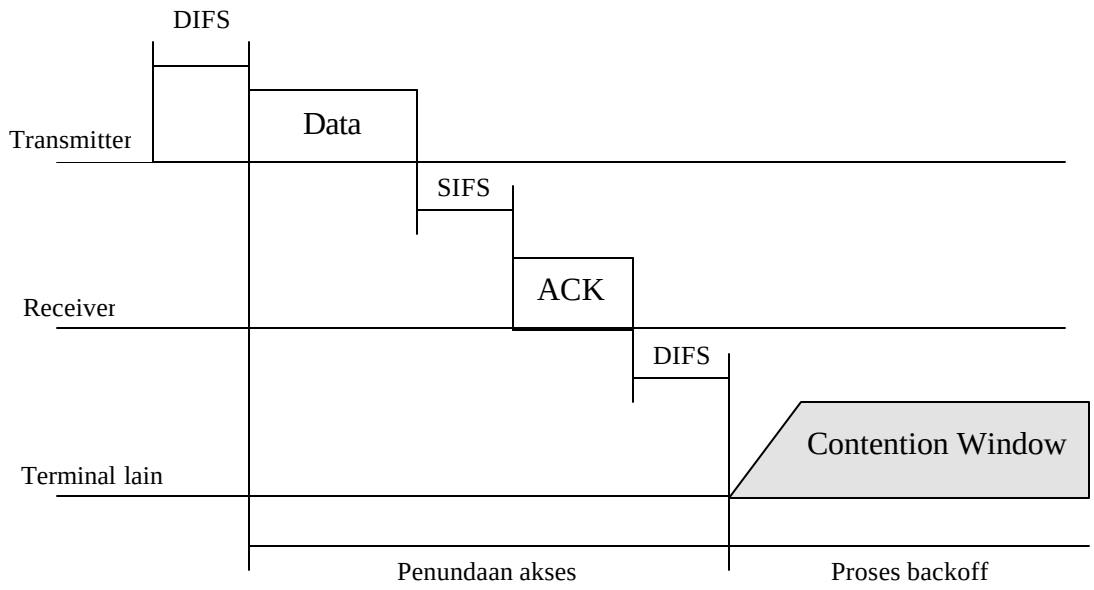
a. *Distributed Coordination Function (DCF).*
b. *Point Coordination Function (PCF).*

##### 3.4.2.1.1. *Distributed Coordination Function (DCF)*

Teknik akses *DCF* disebut dengan Carrier Sense *Multiple* Access with Collision *Avoidance* (*CSMA/CA*), *CSMA/CA* hampir sama dengan sistem deteksi tabrakan data pada *Ethernet (IEEE 802.3).*

Mendeteksi terjadinya tabrakan data pada jaringan *Wireless LAN* tidak mungkin dilakukan karena radio yang digunakan *IEEE 802.11b* adalah radio *half duplex* yang tidak dapat menerima saat mengirim, akibatnya tabrakan tidak bisa dideteksi, inilah alasan mengapa metode menghindari tabrakan data yang digunakan pada *802.11* dan bukannya metode pendeteksian tabrakan data seperti pada *ethernet*.

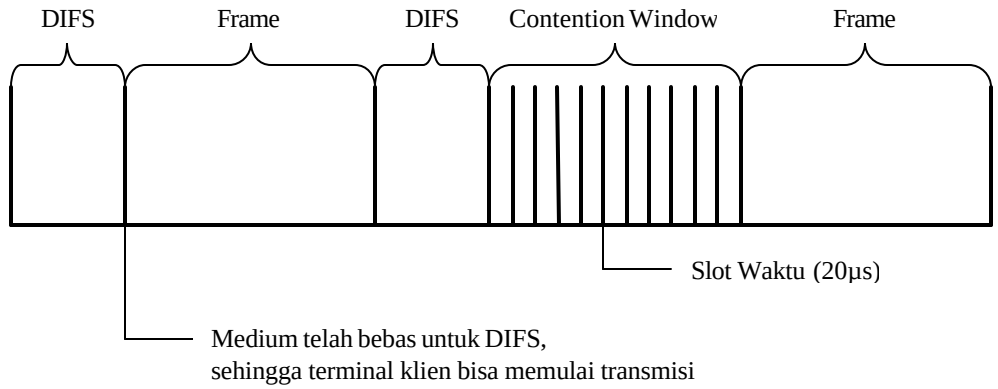
*MAC* menggunakan layanan *CCA* dari *PHY* untuk mengetahui apakah kanal sedang bebas dalam tenggang waktu minimum yang disebut dengan *Distributed Coordination Function (DCF) InterFrame Spacing (DIFS),* jika bebas maka *MAC* akan mentransmisikan paket data, namun jika kanal sibuk *MAC* akan menunggu dengan jalan menghitung mundur waktu yang sama dengan *DIFS* ditambah dengan slot waktu acak untuk kemudian dilakukan fungsi *CCA* lagi, diperlihatkan pada Gambar 3.9.




DIFS : Distributed IFS SIFS : Short IFS ACK : Acknowledgement

Gambar 3.9. *Timeline CSMA/CA*

Tenggang waktu antara akhir dari ***DIFS*** dan awal dari ***frame*** yang selanjutnya disebut dengan ***Contention Window*** yang diperlihatkan pada Gambar 3.10. Durasi setiap slot waktu ditentukan selama 20 mikro detik sehingga sebuah terminal akan selalu dapat menentukan apakah terminal lainnya telah mengakses medium di awal slot sebelumnya.

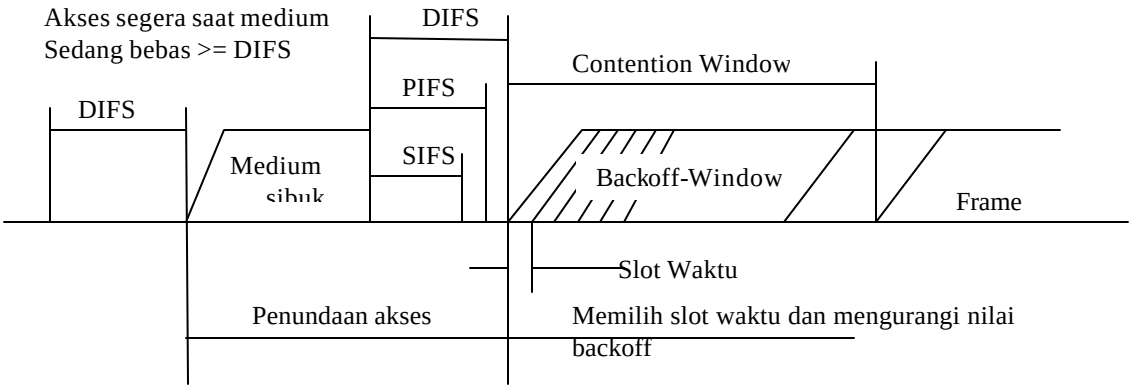



Gambar 3.10. *Contention Window*

Setiap terminal mendengarkan kanal, dan terminal yang pertama kali menyelesaikan slot waktu tunggunya akan mentransmisikan

data, saat terminal lain yang mendengar terminal tersebut mentransmisi menghentikan hitungan mundurnya, saat kanal kembali bebas hitungan mundur dilanjutkan. Setiap terminal mulai menghitung waktu tunda acak hingga nol saat menunggu *contention window*, setiap terminal mendapatkan waktu tunda acak yang baru saat akan mentransmisikan data, pewaktu ini tidak akan di-*reset* hingga terminal telah mentransmisikan data. Ini yang disebut dengan algoritma tunda *(back off algorithm),* tipe akses jamak seperti ini yang membuat pengaturan penggunaan bersama kanal secara adil dan menghindari tabrakan data.

Gambar 3.11. dibawah ini menunjukkan bagaimana mekan*ism*e b*ack* off algorithm ini bekerja:




Gambar 3.11. *Algoritma back off*

Nilai waktu tunda acak maksimum akan meningkat secara signifikan bila pada suatu ketika saat terminal memilih sebuah slot waktu terjadi tabrakan data karena ada terminal lain yang juga aktif, karena itu algoritma *back off* harus dieksekusi pada saat terjadi kasus:

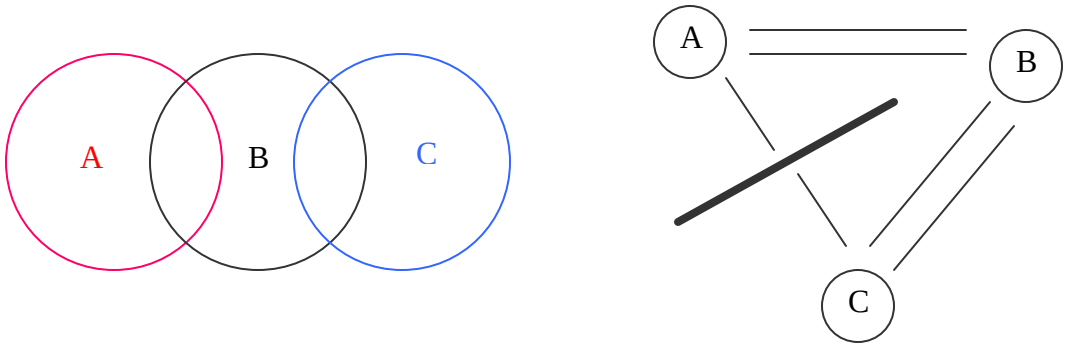
a. Jika terminal memindai medium sebelum transmisi pertama dari paket, dan medium sedang sibuk.
b. Setelah setiap transmisi ulang.
c. Setelah sebuah transmisi terjadi dengan sukses.

Satu-satunya kasus dimana mekan*ism*e ini tidak digunakan adalah saat terminal akan mentransmisikan paket baru dan medium sedang tidak bebas selama lebih dari *DIFS*.

Diantara *frame-frame* kontrol maupun *frame* data *802.11b* terdapat tenggang waktu yang disebut dengan *Inter Frame Spacing (IFS).* Terdapat empat macam *IFS,* dengan prioritasnya masing-masing, yaitu:

1. *Short IFS (SIFS),* digunakan untuk memisahkan setiap *frame* dialog tunggal (misalnya *ACK*), *SIFS* memiliki tenggang waktu yang terkecil yaitu 10 mikro detik, sehingga paling banyak hanya akan ada satu terminal yang akan mentransmisikan paket pada durasi waktu *SIFS,* yang merupakan prioritas tertinggi.
2. *Point Coordination IFS (PIFS)*, digunakan oleh *access point (point koordinator),* untuk memperoleh akses pertama ke medium sebelum terminal lainnya.
   Nilai *PIFS* adalah nilai *SIFS* (10 µS) ditambah dengan satu slot waktu (20 µS) yaitu 30 mikro detik.
3. *Distributed IFS (DIFS), DIFS* adalah *IFS* yang digunakan oleh terminal yang akan memulai transmisi baru, yang nilainya merupakan *PIFS* (30 µS) yang ditambah dengan satu slot waktu(20 µS) yaitu 50 mikro detik.
4. *Extended IFS (EIFS),* adalah *IFS* terpanjang yang digunakan oleh terminal saat menerima paket yang tidak dipahaminya, ini diperlukan untuk mencegah terminal lainnya yang tidak memahami durasi informasi *Virtual Carrier Sense* mengirim paket dan bertabrakan dengan paket selanjutnya dari terminal.

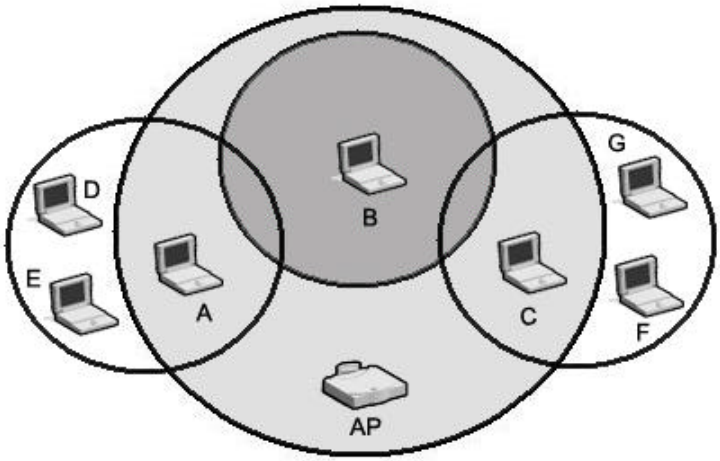
Kekurangan umum dari sistem *Wireless LAN* ialah apa yang disebut dengan *"Hidden Node Problem"* [16], keadaan ini dapat mengganggu komunikasi pada jaringan yang sangat padat. Masalah ini terjadi bila ada terminal pada jaringan yang tidak bisa mendeteksi transmisi dari terminal lainnya untuk mengetahui bahwa medium sedang sibuk seperti Gambar 3.12.




Gambar 3.12. Halangan komunikasi

Pada Gambar di atas diperlihatkan terminal A dan B, C dan B dapat berkomunikasi, tetapi karena tidak memiliki cukup jangkauan jarak atau adanya penghalang membuat terminal A dan C tidak dapat berkomunikasi sehingga terminal C tidak dapat menentukan apakah medium sedang bebas atau tidak, akibatnya terminal A dan C dapat pada waktu yang bersamaan berusaha mengirimkan data pada terminal B.

Protokol *CSMA/CA* memiliki kemampuan untuk mengatasi dan meminimalkan tabrakan data akibat *"Hidden Node Problem"* dengan menggunakan transmisi *frame-frame Request To Send (RTS)*, *Clear To Send (CTS)*, data dan *Acknowledge (ACK)* secara berurutan. Protokol *CSMA/CA* diperlihatkan pada Gambar 3.13.

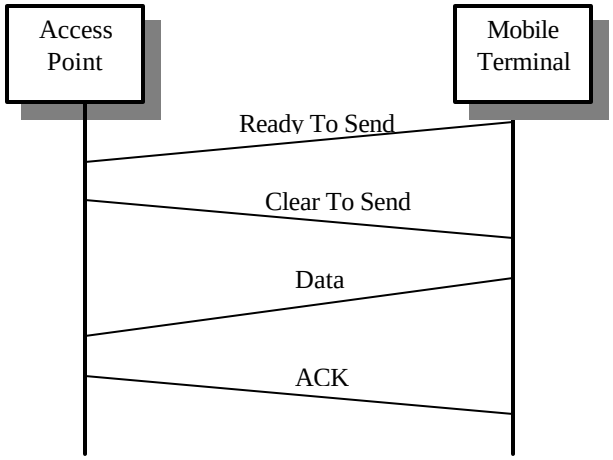



Gambar 3.13. *Hidden node problem*

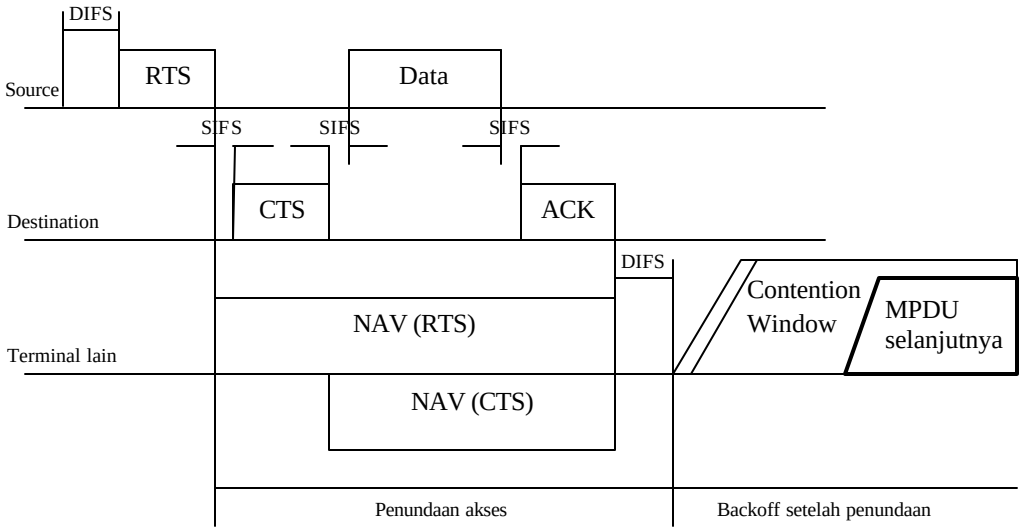
Terlihat terminal A, B dan C kesemuanya dapat berkomunikasi dengan *access point* AP, terminal A dan B, serta B dan C dapat langsung saling berkomunikasi, namun A tidak dapat langsung berkomunikasi dengan C.

Untuk menangani masalah diatas, saat terminal A ingin mentransmisikan data ke B, pertama-tama A mengirimkan paket *RTS* yang berisi alamat tujuan data dan durasi waktu yang akan dibutuhkan untuk transmisi data, paket *RTS* yang kirimkan ini harus sesuai dengan metode pengiriman standar agar dimengerti oleh semua terminal *802.11b*, paket *RTS* ini didengar oleh terminal B, D, dan E, begitu paket *RTS* diterima oleh B, B membalas dengan mengirimkan pesan *CTS* yang berisi lamanya waktu yang akan digunakan untuk transmisi, jika *frame CTS* tidak diterima, maka diasumsikan telah terjadi tabrakan data dan proses *RTS* diulangi lagi, pesan *CTS* yang juga didengar oleh terminal lainnya (C, D, E, F, G) membuat terminal lainnya mengeset indikator *Virtual Carrier Sense*nya (disebut dengan *Network Allocation Vector (NAV)*) yang menyebabkan terminal-terminal tersebut untuk menunda pengiriman datanya dalam tenggang waktu yang cukup untuk mencegah terjadiya tabrakan

data. Setelah paket yang berisi data telah diterima dengan baik (telah dicek nilai *CRC* nya) oleh terminal B, terminal B akan mengirimkan paket *ACK* yang menandakan bahwa transmisi data telah sukses dilakukan, namun bila A tidak menerima paket *ACK* dari B diasumsikan terjadi tabrakan data dan terminal A mengulang transmisi hingga paket *ACK* diterima atau membatalkan transmisi setelah beberapa kali transmisi ulang tidak dibalas dengan paket *ACK.* Setelah paket *ACK* diterima oleh terminal A maka transmisi data dikatakan telah sukses. Urutan proses *handshake CSMA/CA* diperlihatkan pada Gambar 3.14.




Gambar 3.14. *Handshake* [16]




Gambar 3.15. *CSMA/CA*

Jika semua terminal dalam jaringan nirkabel menggunakan teknik *CSMA/CA* [13] seperti pada Gambar 3.15., maka diyakini bahwa tabrakan data hanya terjadi di dalam *Contention Window*. *Access point* dapat ikut berpartisipasi dalam proses *CSMA/CA* ini jika dibutuhkan. Teknik *CSMA/CA* ini meningkatkan kepadatan lalu lintas data dalam jaringan *802.11*, karena itu jika protokol ini digunakan nilai-nilai untuk pengaturan pewaktuan harus diset dengan baik pada *access point* maupun pada *adapter Wireless LAN*.

Meskipun begitu, perlu diingat bahwa *RTS* dan *CTS* adalah paket *frame* yang kecil sehingga mengurangi waktu yang dibutuhkan untuk transmisi jika yang bertabrakan adalah paket data yang besar, karena itu untuk paket-paket data yang kecil dapat ditransmisikan tanpa menggunakan protokol *CSMA/CA*, ini diatur dengan mengubah parameter *RTS Threshold* pada masing-masing terminal.

#### 3.4.2.1.2.*Point Coordination Function (PCF)*

*PCF* hanya digunakan untuk mengakomodasi transmisi yang terikat dengan waktu/*connection oriented* seperti transmisi suara dan video, ini dilakukan dengan prioritas yang lebih tinggi pada penggunaan *access point*, yaitu penggunaan *IFS* yang lebih kecil.

Dengan penggunaan prioritas yang lebih tinggi ini, *access point* mengontrol medium dan meminta transmisi data dari terminal. Agar terminal lainnya masih dapat mengakses medium, diatur agar *access point* tetap menyisakan cukup waktu untuk akses *DCF* disela-sela penggunaan *PCF*.

### 3.4.2.2. *Cyclic Redundancy Check (CRC)* [4]

*Cyclic Redundancy Check (CRC)* berfungsi untuk memeriksa paket data yang diterima apakah rusak dalam pengiriman, setiap paket data memiliki *CRC* yang dihitung dan disertakan dalam transmisi. *CRC* sangat berguna dalam mendeteksi baik kesalahan bit tunggal maupun banyak bit.

Secara teoritis *CRC* dapat dianggap dengan membagi data biner dengan bilangan biner yang tetap (sering juga disebut dengan polinomial), dan sisa hasil baginya merupakan *checksum* yaitu *CRC* yang disertakan dalam paket pengiriman data.

Algoritma *CRC* yang digunakan pada standar *802.11* adalah *CCITT CRC 16*, yang disahkan oleh badan standar *Comite Consultatif Internationale de Telegraphique et Telephonique (CCITT).*

### 3.4.2.3. Keamanan [17]

*MAC 802.11b* juga memiliki metode untuk mengamankan data yang disebut dengan *Wired Equivalent Privacy (WEP)*. *WEP* bekerja dengan jalan mengenkripsi data yang ditransmisikan dengan kunci sepanjang 64 atau 128 bit menggunakan algoritma *RSA RC4*.

*WEP* akan dijelaskan secara lebih detil dan mendalam pada bab 4 dari tugas akhir ini.

### 3.4.2.4. Fragmentasi dan Penggabungan Data [14]

Fragmentasi paket akan memecah paket yang besar menjadi paket-paket yang lebih kecil saat dikirimkan melalui gelombang radio. Ini memiliki dua keuntungan, yaitu mengurangi kebutuhan untuk transmisi ulang karena kemungkinan terjadi kerusakan paket semakin besar bila ukuran paket semakin besar dan jika terjadi kerusakan paket pengirim hanya perlu mentransmisikan ulang paket yang rusak saja, sehingga lebih cepat.

Protokol *LAN* biasa menggunakan paket-paket yang panjangnya hanya beberapa ratus *bytes,* pada lingkungan *Wireless LAN* terdapat beberapa alasan kenapa digunakan paket-paket yang berukuran kecil:

a. Karena tingginya *Bit Error Rate (BER)* pada komunikasi radio, sehingga kemungkinan terjadinya kerusakan paket lebih besar dengan bertambah besarnya ukuran paket.
b. Pada kasus terjadinya kerusakan paket baik oleh tabrakan data atau derau, paket yang ukurannya kecil memiliki waktu lebih sedikit untuk mentransmisi ulang.
c. Pada sistem *FHSS* dimana frekuensi terus berubah-ubah, ukuran paket yang lebih kecil membuat kemungkinan transmisi tertunda lebih kecil.

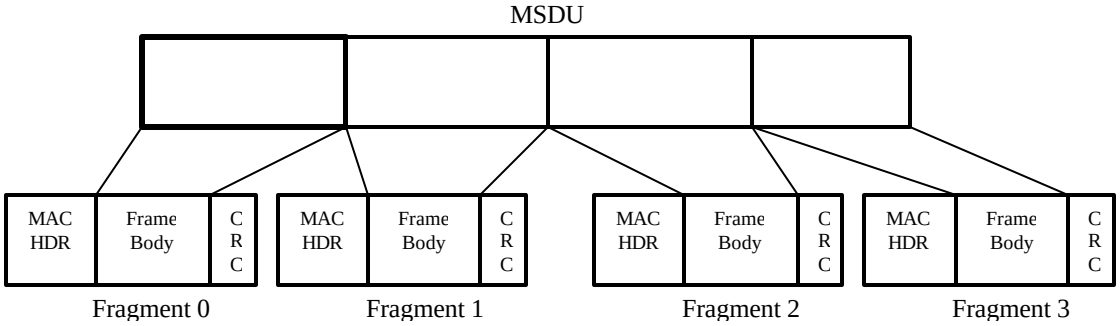
Disisi lain, akan tidak masuk akal bila dibuat protokol *LAN* baru yang tidak dapat menangani ukuran paket sebesar 1518 *byte* yang digunakan pada *ethernet*, karena itu digunakan pemecahan masalah dengan menambahkan fungsi fragmentasi dan penggabungan data sederhana di *layer MAC*.

Mekanisme ini merupakan algoritma kirim dan tunggu (*Send and Wait Algorithm*) yang sederhana, dimana terminal yang melakukan transmisi suatu bagian dari data dilarang mengirimkan bagian yang lainnya hingga salah satu dibawah ini terjadi:

1. Menerima *frame ACK* dari bagian yang telah dikirim.
2. Membatalkan transmisi karena transmisi ulang telah dilakukan berkali-kali tanpa ada balasan *frame ACK*.

*MAC* tidak memperbolehkan suatu terminal untuk mentransmisikan paket ke alamat yang lain pada saat sedang melakukan transmisi ulang suatu bagian paket, ini berguna saat *access point* memiliki beberapa paket yang menunggu untuk dikirimkan ke beberapa tujuan, sedangkan salah satu tujuan tidak merespon.

Dibawah ini diperlihatkan Gambar 3.16., sebuah *frame MAC Service Data Units (MSDU)* yang dibagi menjadi beberapa bagian *MAC Protocol Data Units (MPDU)*:




Gambar 3.16. *MSDU*

## 3.5. Teknik Modulasi [4]

Teknik modulasi yang digunakan oleh standar *IEEE 802.11* adalah *Differential Binary Phase Shift Keying (DBPSK)* untuk kecepatan 1 Mbps dan *Differential Quadrature Phase Shift Keying (DQPSK)* untuk kecepatan 2 Mbps, sedangkan pada standar *IEEE 802.11b* ditambahkan teknik modulasi *Complementary Code Keying (CCK)* untuk kecepatan 5.5 Mbps dan 11 Mbps, dengan pilihan penggunaan modulasi *Packet Binary Convolution Coding (PBCC)* dimungkinkan untuk peningkatan performa. Agar kompatibel dengan generasi *802.11* yang lama, *802.11b* dapat menurunkan kecepatan transfer ke 5.5 Mbps, 2 Mbps atau 1 Mbps secara otomatis yang disesuaikan dengan kondisi jarak, interferensi, derau, kekuatan sinyal atau jika berkomunikasi dengan *adapter 802.11.*

Deretan bit-bit *11 chip Barker sequence* yang digunakan untuk modulasi 1 Mbps dan 2 Mbps adalah:

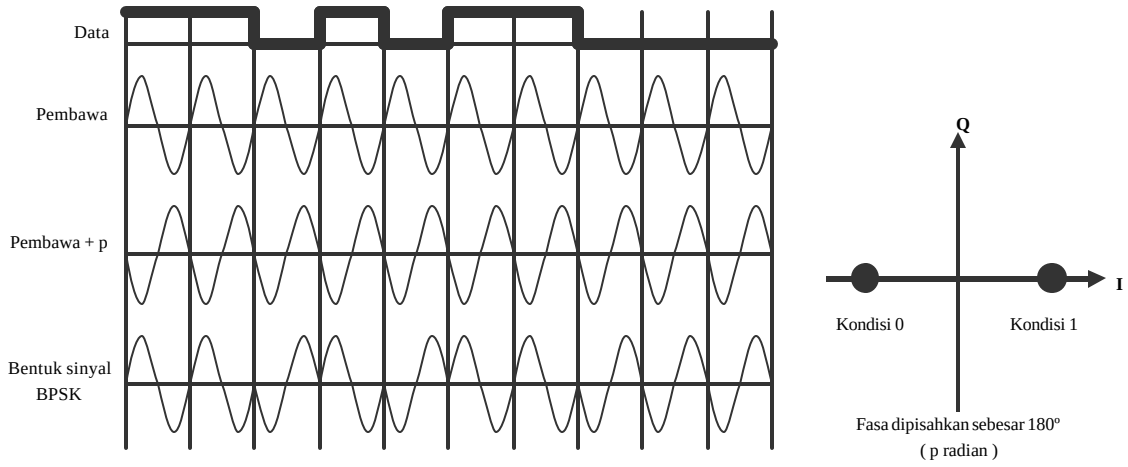
+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

*Chip* yang ada paling kiri harus menjadi keluaran terlebih dahulu, *chip* yang pertama tersebut harus disejajarkan pada awal mula transmisi, panjang simbol harus tepat *11 chip*.

### 3.5.1. *Differential Binary Phase Shift Keying (DBPSK)*

Disebut *Binary PSK* karena hanya ada dua keadaan biner. Disini data “1” diwakili oleh polaritas positif (+90°) dan data “0” diwakili oleh polaritas negatif (-90°), sehingga kedua polaritas ini memiliki perbedaan fasa sebesar 180°. Digambarkan pada Gambar 3.17.

Secara teoritis, perpindahan dari “1” ke “0” dan sebaliknya menghasilkan perubahan fasa yang tajam sehinga lebar pitanya menjadi tak terhingga, namun pada prakteknya tidaklah demikian karena akan terjadi penghalusan pada saat transmisi.




Gambar 3.17. *DBPSK*

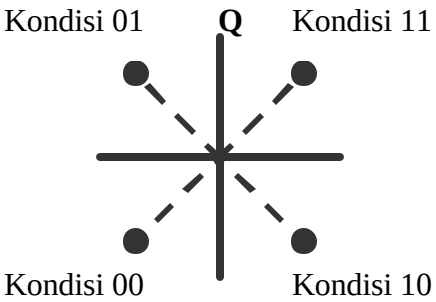
Tabel enkoder untuk *DBPSK* terlihat pada Tabel dibawah ini:

Tabel 3.4. *DBPSK*

| Bit masukan | Perubahan Fase (+j?) |
|---|---|
| 0 | 0 |
| 1 | ? |

### 3.5.2. *Differential Quadrature Phase Shift Keying (DQPSK)*

Disebut *Quadrature PSK* karena memiliki empat keadaan biner. *DQPSK* sanggup memberikan dua bit informasi sekaligus karena pergeseran fasa yang diberikan adalah empat buah, yaitu +135°, +45°, -45°, -135°, terlihat Gambar 3.18. Jadi setiap data mengandung dua bit informasi.




Bentuk Sinyal keluaran adalah hasil penjumlahan sinyal Cosinus ± dan Sinus ± yang dimodulasi

Fasa pembawa :
p/4, 3p/4, 5p/4, 7p/4
Memiliki efisiensi 2x lipat dari BPSK

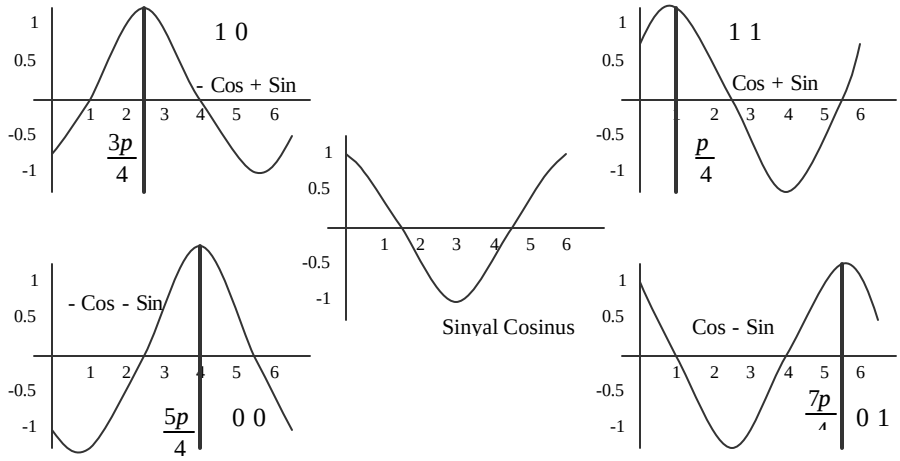
Gambar 3.18. *DQPSK*

Enkoder untuk *DQPSK* ditabelkan dibawah ini:

Tabel 3.5. *DQPSK*

| Pola bit (d0,d1)<br>(d0 yang pertama sebagai f(t)) | Perubahan Fase (+j?) |
|---|---|
| 00 | 0 |
| 01 | ?/2 |
| 11 | ? |
| 10 | 3 ?/2 (-?/2) |

Bentuk sinyal keluaran yang berupa penjumlahan antara sinyal Cosinus ± dan Sinus ± yang dimodulasi ditampilkan pada Gambar 3.19.:




Gambar 3.19. Penjumlahan sinus dan cosinus

### 3.5.3. *Complementary Code Keying (CCK)*

*CCK* tetap menggunakan chip dengan kecepatan 11 Mchips/s, namun panjang deretan bit yang digunakan hanyalah 8 bit, kedelapan bit tersebut membentuk sebuah simbol, dan dengan kecepatan simbol sebesar 1375 Msymbols/s membuat transmisi data 11 Mbps cukup untuk dilewatkan pada lebar pita yang hanya cukup untuk melewatkan 2 Mbps dengan menggunakan modulasi *QPSK*. Sedangkan untuk kecepatan transmisi 5.5 Mbps hanya digunakan panjang deretan 4 bit saja. Ini penting untuk memaksimalkan transfer data pada jaringan *Wireless LAN* dan merupakan salah satu alasan mengapa digunakan teknik modulasi *CCK*.

Kedelapan bit tersebut berguna untuk mengkodekan parameter-parameter f menurut Tabel 3.6. dibawah ini:

Tabel 3.6. Parameter fasa

| Dibit | Parameter fasa |
|---|---|
| (d1,d0) | F1 |
| (d3,d2) | F2 |
| (d5,d4) | F3 |
| (d7,d6) | F4 |

Setelah diperoleh nilai fasa, kemudian bisa diperoleh nilai bit-bit data dengan jalan menggunakan Tabel enkoder modulasi *DQPSK* 3.4. diatas.

Sedangkan untuk penggunaan kecepatan transfer 5.5 Mbps digunakan Tabel enkoder 3.7. dibawah ini:

Tabel 3.7. Dekoder untuk 5.5 Mbps

| d2,d3 | c1 | c2 | c3 | c4 | c5 | c6 | c7 | C8 |
|---|---|---|---|---|---|---|---|---|
| 00 | 1j | 1 | 1j | -1 | 1j | 1 | -1j | 1 |
| 01 | -1j | -1 | -1j | 1 | 1j | 1 | -1j | 1 |
| 10 | -1j | 1 | -1j | -1 | -1j | 1 | 1j | 1 |
| 11 | 1j | -1 | 1j | 1 | -1j | 1 | 1j | 1 |

### 3.5.4. *Packet Binary Convolution Coding (PBCC)*

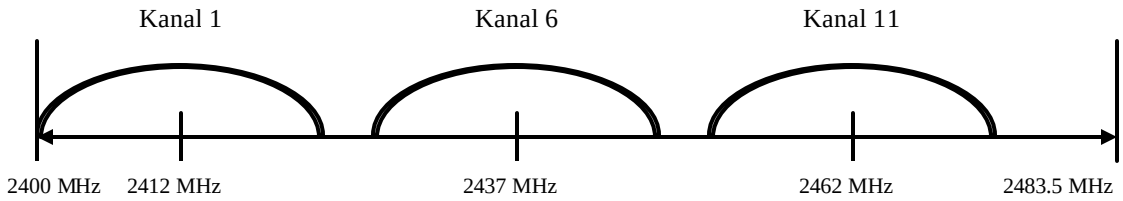
Teknik modulasi tambahan ini menggunakan 64 posisi pengkodean konvolusi biner/*Binary Convolutional Code (BCC)* dengan sederetan data sampul. Keluaran dari *BCC* kemudian dipetakan ke dalam bentuk posisi modulasi menggunakan dua macam kemungkinan kecepatan, 5.5 Mbps dengan *BPSK* dan 11 Mbps dengan *QPSK*.

### 3.6. Kanal Operasi [4]

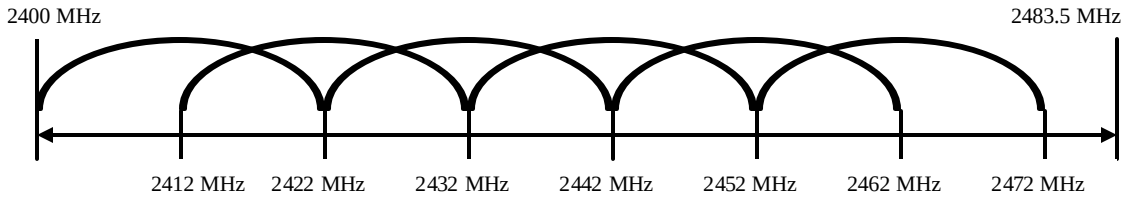
Kanal untuk beroperasi ditentukan oleh peraturan pada masing-masing negara, diberikan:

Tabel 3.8. Kanal operasi Amerika Utara

| Set | Jumlah kanal | Nomor kanal *DSSS* |
|---|---|---|
| 1 | 3 | 1, 6, 11 |
| 2 | 6 | 1, 3, 5, 7, 9, 11 |



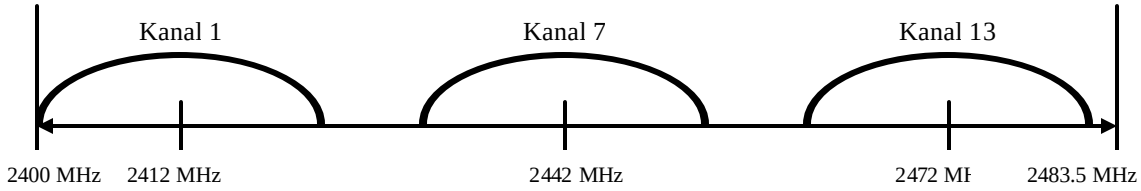

Gambar 3.20. Pemilihan kanal Amerika utara (tidak *overlap*)



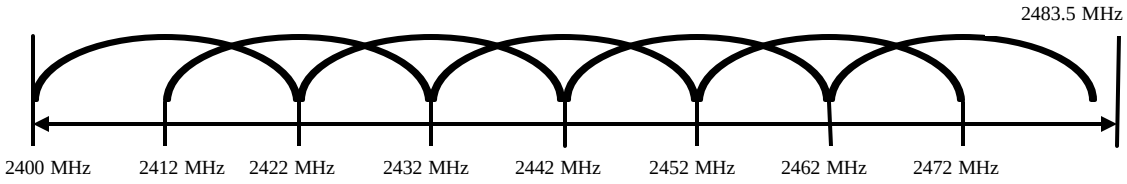

Gambar 3.21. Pemilihan kanal Amerika Utara (*overlap*)

Tabel 3.9. Kanal operasi Eropa kecuali Perancis dan Spanyol

| Set | Jumlah kanal | Nomor kanal *DSSS* |
|---|---|---|
| 1 | 3 | 1, 7, 13 |
| 2 | 7 | 1, 3, 5, 7, 9, 11, 13 |




Gambar 3.22. Pemilihan kanal Eropa (tidak *overlap*)




Gambar 3.23. Pemilihan kanal Eropa (*overlap*)

Untuk banyak kanal dapat berada bersamaan di suatu lokasi, setiap kanal harus terpisah sejauh 25 Mhz satu sama lain untuk menghindari interferensi, ini artinya maksimum hanya tiga kanal *Wireless LAN* dapat berada bersamaan di suatu tempat.

### 3.7. Penghematan Tenaga [15]

Saat beroperasi dengan normal, *adapter 802.11b* menggunakan teknik *Constant Access Mode (CAM),* yaitu secara terus menerus mendengarkan/memindai jaringan dan menerima data yang dibutuhkannya. Namun saat dibutuhkan penghematan tenaga, misalnya penggunaan baterai pada komputer portabel, maka terminal dan akses point dapat dikonfigurasi untuk menggunakan mode yang disebut dengan *Polled Access Mode (PAM).*

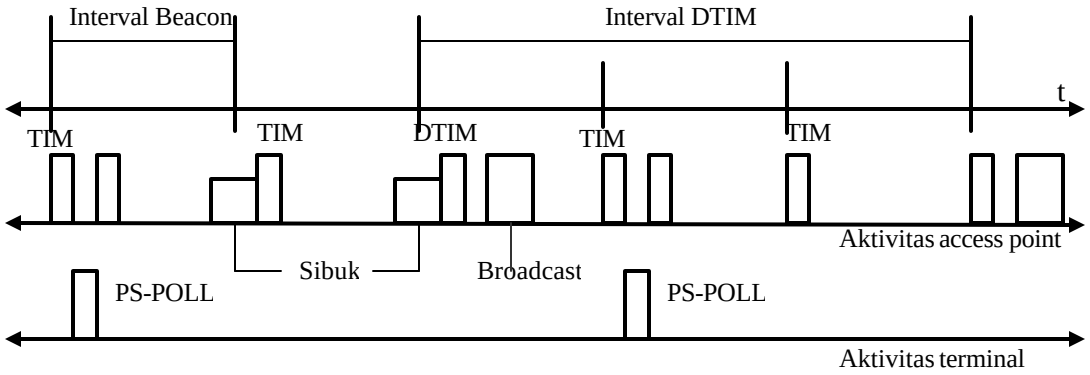
Dengan teknik *PAM* ini semua terminal pada jaringan hanya aktif/“bangun” pada periode waktu tertentu untuk mendengarkan paket-paket data khusus dari *access point* yang disebut dengan *Traffic Information Map (TIM).* Disela-sela waktu *TIM* tersebut terminal-terminal mematikan radionya/“tidur” sehingga

menghemat energi, semua terminal didalam jaringan harus aktif pada waktu yang tepat bersamaan untuk bisa mendengarkan paket *TIM* dari *access point*.

Paket *TIM* berisi informasi yang memberitahu terminal-terminal tertentu bahwa mereka memiliki data yang disimpan sementara di *access point* dan menunggu untuk dikirimkan, terminal yang diberitahu kemudian tetap aktif untuk menerima data dari *access point* hingga semua data telah ditransfer ke terminal, dan kemudian terminal kembali “tidur”.

*Access point* menyimpan sementara/mem-*buffer* semua data untuk setiap terminal hingga menerima permintaan pengiriman dari terminal tujuan data. Setelah data dikirimkan, terminal kembali ke dalam mode penghematan tenaga hingga paket *TIM* selanjutnya dikirimkan. Teknik penghematan tenaga ini dapat menghemat energi yang digunakan oleh terminal bergerak, namun tergantung pula pada kepadatan lalu lintas jaringan.

*Access point* memberitahu seluruh terminal dalam jaringan akan adanya lalu lintas data *TIM* dengan menggunakan paket *Delivery Traffic Information Map (DTIM),* pewaktu *DTIM* selalu merupakan kelipatan dari pewaktu *TIM* dan dapat diset di *access point*, menggunakan nilai *DTIM* yang besar mengurangi jumlah total waktu yang dibutuhkan oleh terminal untuk tetap “bangun” dan mengecek lalu lintas jaringan, namun nilai *DTIM* yang besar akan membuat radio menyala lebih lama saat menerima lalu lintas data *DTIM* saat paket ini disiarkan dijaringan dalam setiap periode waktu, diperlihatkan pada Gambar 3.24.




Gambar 3.24. *Timing Beacon* pada mode *power saving*

### 3.8. Sinkronisasi [14]

Terminal-terminal dan *access point* perlu untuk selalu menjaga sinkronisasi diantara mereka, pada sistem *FHSS* ini diperlukan untuk menyamakan pola loncatan frekuensi, sedangkan untuk sistem *DSSS* digunakan untuk penghematan tenaga. Sinkronisasi dilakukan dengan jalan semua terminal menyesuaikan jam mereka dengan jam yang ada di *access point*, menggunakan mekan*ism*e berikut:

*Access point* mentransmisikan secara periodik *frame-frame* yang disebut dengan *Beacon Frames*, *frame* ini berisi nilai waktu yang ada pada jam *access point* saat transmisi itu, ini adalah waktu dimana transmisi benar-benar terjadi, bukan saat suatu transmisi dimasukkan ke daftar tunggu transmisi, karena pada sistem akses *CSMA/CA* suatu transmisi dapat tertunda secara signifikan.

Terminal penerima *beacon frames* mengecek nilai jam mereka pada saat penerimaan, kemudian menyesuaikannya agar selalu sinkron dengan jam dari *access point*, ini mencegah agar jam tidak bergeser yang dapat menyebabkan hilangnya sinkronisasi setelah beroperasi selama beberapa jam.

### 3.9. Otentikasi dan Asosiasi [14]

Saat sebuah terminal ingin mengakses sebuah jaringan komputer nirkabel, baik setelah dinyalakan atau dari kondisi "tidur", maupun karena telah memasuki daerah jangkauan *Wireless LAN*, terminal harus mencari informasi sinkronisasi dari *access point* atau dari terminal yang lainnya. Ini dapat dilakukan dengan menggunakan 2 metode:

1. Memindai secara pasif (*Passive Scanning*), dalam hal ini terminal hanya menunggu untuk menerima *beacon frame* yang disebarkan secara periodik oleh *access point*.
2. Memindai secara aktif (*Active Scanning*), dalam hal ini terminal mencoba mencari *access point* dengan mengirimkan *frame* pemindai/*Probe Request Frames,* dan menunggu respon dari *access point* berupa *Probe Response*.

Kedua metode diatas dapat digunakan salah satu tergantung pada perbandingan antara performa dan konsumsi tenaga.

#### 3.9.1. Proses Otentikasi

Setelah terminal menemukan *access point* dan memutuskan akan masuk ke dalam jaringan, terminal akan menjalani proses otentikasi yaitu proses pertukaran informasi antara *access point* dan terminal, dimana kedua belah pihak mencocokkan password.

Ini dilakukan dengan menggunakan prosedur *challenge response* dan kunci rahasia. Setelah sebuah terminal meminta untuk diotentikasi, pengotentikasi mengirimkan *challenge* berupa angka acak sepanjang 128 oktet, terminal mengenkripsi *challenge* tersebut menggunakan kunci rahasia dan mengirimkannya kembali ke otentikator untuk diverifikasi.

### 3.9.2. Proses Asosiasi

Setelah terminal di otentikasi, terminal akan memulai proses asosiasi yang merupakan proses pertukaran informasi tentang kemampuan dari terminal dan jaringan agar *access point* mengetahui lokasi dari terminal. Setelah proses asosiasi selesai barulah terminal diperbolehkan mengirim dan menerima data.

## 3.10. Berbagai Tipe *Frame 802.11b* [14]

*Frame* digolongkan ke dalam tiga jenis utama:

2. *Frame* data, yang digunakan untuk transmisi data.
2. *Frame* kontrol, digunakan untuk mengakses kontrol terhadap medium, contohnya *RTS, CTS*, dan *ACK*.
2. *Frame* manajemen, merupakan *frame* yang ditransmisikan dengan cara yang sama seperti *frame* data untuk bertukar informasi manajemen, tetapi tidak diteruskan ke lapisan *layer* atas.

Masing-masing tipe *frame* dibagi lagi menjadi beberapa subtipe yang disesuaikan dengan fungsi-fungsi spesifiknya.

### 3.10.1. Format *Frame PHY 802.11b*

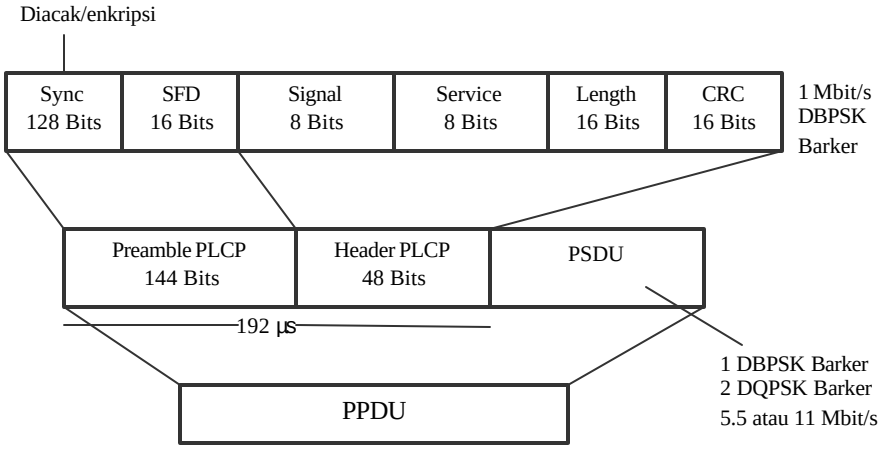
Semua *frame* data dari *802.11* terdiri atas komponen-komponen:


Gambar 3.25. *Frame 802.11*

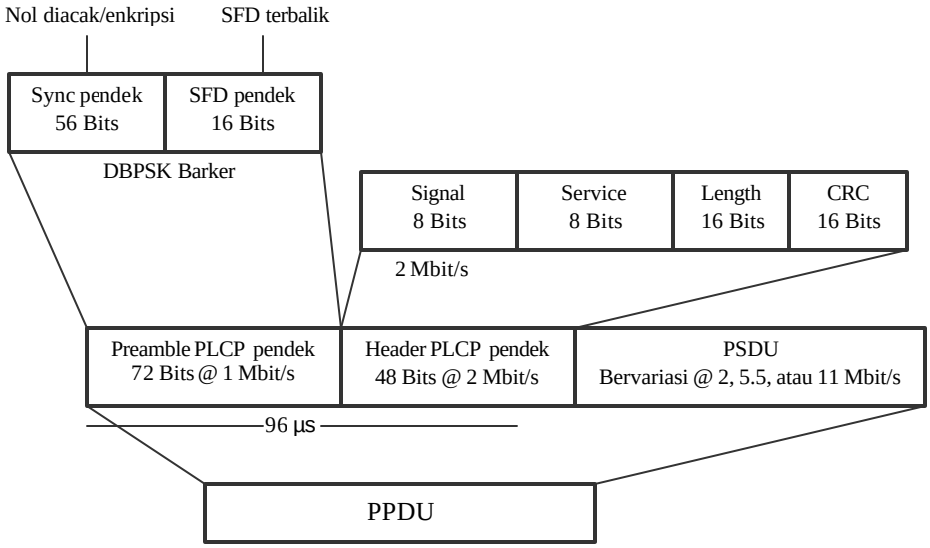
*PLCP* memiliki dua macam struktur/format data, *PLCP PPDU* panjang dan pendek, semua sistem *802.11b* harus mensupport format *PLCP PPDU* panjang sedangkan *PLCP PPDU* pendek disediakan untuk meningkatkan efisiensi jaringan saat mentransmisikan

data-data khusus seperti suara, *Voice Over IP (VoIP)*, dan video *streaming.*

Format *frame PLCP PPDU:*




Gambar 3.26. Format *PLCP PPDU* panjang




Gambar 3.27. Format *PLCP PPDU* pendek

*PLCP PPDU* terdiri atas *preamble* sepanjang 144 bit yang digunakan untuk sinkronisasi dalam menentukan kekuatan sinyal radio dan melaksanakan *CCA, preamble* dari *PLCP*:

a. Bagian sinkronisasi sepanjang 128 bit untuk *PLCP* panjang dan 56 bit untuk *PLCP* pendek.

b. 16 bit bagian *Start Frame Delimiter (SFD)* sebagai tanda awal dari semua *frame*, pola *SFD* selalu sama yaitu 1 1 1 1 0 0 1 1 1 0 1 0 0 0 0 0.

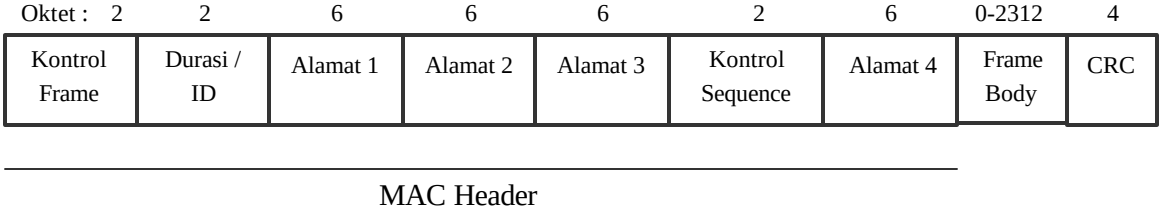
48 bit setelah *preamble* merupakan bagian yang disebut dengan *PLCP header*, *header* terdiri dari empat bagian:

a. 8 bit bagian *Sinyal* atau *Data Rate (DR)* yang mengindikasikan seberapa cepat data akan ditransmisikan, apakah 1, 2, 5.5, atau 11 Mbps.
b. 8 bit bagian *Service* disediakan untuk penggunaan masa depan.
c. 16 bit bagian *Length* untuk menunjukkan panjang dari *Protocol Data Unit (PDU) MAC* yang berikutnya.
d. 16 bit bagian pengecekan kesalahan *Cyclic Redundancy Code (CRC)* dari *header, Header Error Check (HEC).*

*Preamble* pendek *PLCP* harus ditransmisikan menggunakan kecepatan 1 Mbps dengan modulasi *DBPSK*, sedangkan *header* pendek *PLCP* harus ditransmisikan menggunakan modulasi 2 Mbps.

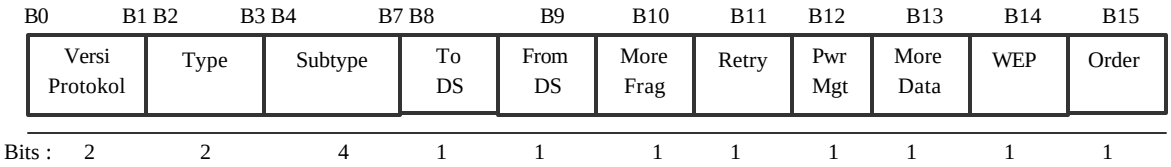
### 3.10.2. Format *Frame* Data *MAC 802.11b*

Secara umum format *frame* data dari *MAC* digambarkan dibawah ini, setiap bagian darinya merupakan *frame-frame* tersendiri yang akan dijelaskan nanti.




Gambar 3.28. Format *frame MAC*

Bagian kontrol *frame* terdiri atas:




Gambar 3.29. Format kontrol *frame*

1. *Protocol Version/*Versi Protokol

   Bagian ini terdiri atas 2 bit yang letak dan ukurannya selalu tetap pada berbagai macam versi standar *802.11,* digunakan untuk mengenali versi-versi standar *802.11.*

2. *Tipe* dan *subtipe*

   Bagian yang terdiri atas 6 bit ini mendefinisikan tipe dan subtipe *frame* yang ditabelkan:

Tabel 3.10. Tipe dan subtipe

| Nilai tipe b3,b2 | Deskripsi tipe | Nilai subtipe b7,b6,b5,b4 | Deskripsi subtipe |
|---|---|---|---|
| 00 | Manajemen | 0000 | Permintaan asosiasi |
| 00 | Manajemen | 0001 | Tanggapan asosiasi |
| 00 | Manajemen | 0010 | Permintaan reasosiasi |
| 00 | Manajemen | 0011 | Tanggapan reasosiasi |
| 00 | Manajemen | 0100 | Permintaan *probe* |
| 00 | Manajemen | 0101 | Tanggapan *probe* |
| 00 | Manajemen | 0110 - 0111 | Dikosongkan |
| 00 | Manajemen | 1000 | *Beacon* |
| 00 | Manajemen | 1001 | *ATIM* |
| 00 | Manajemen | 1010 | Dis-asosiasi |
| 00 | Manajemen | 1011 | Otentikasi |
| 00 | Manajemen | 1100 | Dis-otentikasi |
| 00 | Manajemen | 1101 – 1111 | Dikosongkan |
| 01 | Kontrol | 0000 – 1001 | Dikosongkan |
| 01 | Kontrol | 1010 | *PS-Poll* |

| | | | |
|---|---|---|---|
| 01 | Kontrol | 1011 | *RTS* |
| 01 | Kontrol | 1100 | *CTS* |
| 01 | Kontrol | 1101 | *ACK* |
| 01 | Kontrol | 1110 | *CF End* |
| 01 | Kontrol | 1111 | *CF End + CF–ACK* |
| 10 | Data | 0000 | *Data* |
| 10 | Data | 0001 | *Data + CF-Ack* |
| 10 | Data | 0010 | *Data + CF-Poll* |
| 10 | Data | 0011 | *Data+CF-Ack+CF-Poll* |
| 10 | Data | 0100 | Fungsi Null(Tanpa data) |
| 10 | Data | 0101 | *CF-Ack* (Tanpa Data) |
| 10 | Data | 0110 | *CF-Poll* (Tanpa Data) |
| 10 | Data | 0111 | *CF-Ack+CF-Poll* (Tanpa data) |
| 10 | Data | 1000 – 1111 | Dikosongkan |
| 11 | Dikosongkan | 0000 - 1111 | Dikosongkan |

3. *ToDS*

   Bit ini diset ke “1” bila *frame* ditujukan ke *access point* untuk diteruskan ke *Distribution System (DS),* termasuk jika *frame* ditujukan ke terminal lainnya dalam jaringan, dan *access point* berfungsi sebagai pe-*relay frame.*

   Untuk *frame-frame* lainnya bit ini diset ke “0”.

   *Distribution System (DS)* merupakan hubungan *LAN* antar *access point* yang membentuk semacam *backbone* komunikasi antara jaringan nirkabel yang satu dengan yang lainnya.

4. FromDS

   Bit ini diset ke “1” saat *frame* datang dari *Distribution System (DS).*

5. *More Fragments*

   Bit ini diset ke “1” saat masih ada fragmen lainnya yang merupakan bagian dengan *frame* yang diterima.

6. *Retry*

   Bit ini mengindikasikan bahwa fragmen ini merupakan transmisi ulang dari fragmen yang sebelumnya telah dikirimkan, ini digunakan oleh terminal penerima untuk mengenali transmisi *frame* yang diulang akibat hilangnya paket data atau paket *acknowledgement (ACK).*

7. Manajemen tenaga

   Bit ini menunjukkan mode dari manajemen tenaga yang akan digunakan oleh terminal setelah transmisi *frame* ini. Digunakan oleh terminal yang akan berganti status, baik dari *PAM* ke *CAM* maupun sebaliknya.

8. *More Data*

   Bit ini juga digunakan untuk manajemen tenaga dan digunakan oleh *access point* untuk mengindikasikan bahwa masih ada *frame* selanjutnya yang disimpan sementara untuk terminal. Terminal kemudian menentukan apakah mereka akan tetap mendengarkan atau berganti status ke *CAM.*

9. *WEP*

   Bit *WEP* digunakan untuk mengindikasikan bahwa *frame* body dienkripsi dengan algoritma *WEP.*

10. *Order*

    Bit ini mengindikasikan bahwa *frame* tersebut dikirim menggunakan *Strictly Ordered Service Class*, yaitu definisi yang digunakan untuk terminal yang tidak bisa menerima perubahan urutan antara *frame-frame unicast* dan *multicast* karena urutan *frame unicast* ke tujuan tertentu selalu dipertahankan.

11. Durasi/*ID*

    Bagian *frame* ini memiliki dua makna, tergantung dari tipe *frame*nya, pada mode *PAM* bagian ini berisi identitas terminal/*terminal ID*, sedangkan pada *frame* lainnya berisi nilai durasi yang digunakan pada perhitungan *NAV.*

12. Bagian alamat

Sebuah *frame* dapat berisi hingga empat alamat, tergantung pada bit-bit *ToDS* dan *FromDS* yang didefinisikan pada bagian kontrol, masing-masing alamat tersebut:

a. Alamat pertama, selalu merupakan alamat penerima, yaitu stasiun yang menerima *frame*. Jika bit *ToDS* diset maka bagian ini berisi alamat *access point*, sedangkan jika tidak diset bagian ini berisi alamat terminal tujuan akhir.
b. Alamat kedua, selalu merupakan alamat pengirim, yaitu stasiun yang mentransmisikan *frame*. Jika nilai *FromDS* diset maka bagian ini berisi alamat *access point*, jika tidak diset bagian ini berisi alamat terminal.
c. Alamat ketiga, pada kebanyakan kasus bagian ini berisi alamat yang hilang. Pada *frame* dengan *FromDS* diset ke “1” bagian ini berisi alamat pengirim yang sebenarnya, dan jika *ToDS* diset maka bagian ini berisi alamat tujuan.
d. Alamat keempat, digunakan pada keadaan khusus dimana *Distribution System (DS)* digunakan, dan *frame* ditransmisikan antar *access point*, pada keadaan ini baik *ToDS* dan *FromDS* diset sehingga alamat tujuan dan pengirim yang asli hilang.

Tabel 3.11. dibawah ini menunjukkan penggunaan pengalamatan yang berbeda tergantung pada pengaturan *ToDS* dan *FromDS.*

Tabel 3.11. Alamat

| *ToDS* | *FromDS* | Alamat 1 | Alamat 2 | Alamat 3 | Alamat 4 |
|---|---|---|---|---|---|
| 0 | 0 | *DA* | *SA* | *BSSID* | Kosong |
| 0 | 1 | *DA* | *BSSID* | *SA* | Kosong |
| 1 | 0 | *BSSID* | *SA* | *DA* | Kosong |
| 1 | 1 | *RA* | *TA* | *DA* | *SA* |

13. *Sequence Control*

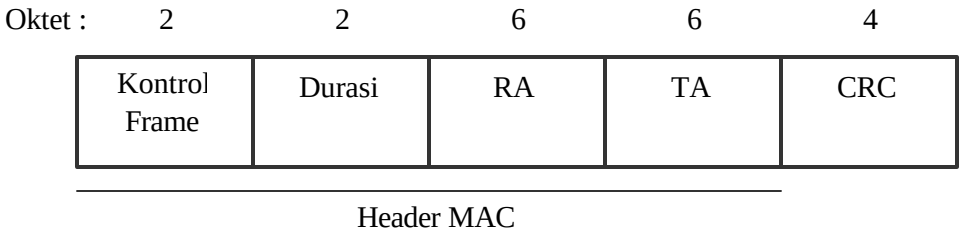
Bagian *sequence kontrol* digunakan untuk menunjukkan urutan fragmen-fragmen yang berasal dari *frame* yang sama, dan untuk mengenali paket yang dikirim ulang. Bagian ini terdiri dari dua sub bagian, yaitu *Fragment Number d*an *Sequence Number*, yang mendefinisikan nomor urutan fragmen dan jumlahnya dalam *frame.*

14. *CRC*

*CRC* adalah bagian yang berisi 16 bit *Cyclic Redundancy Check (CRC)* untuk pengecekan kesalahan dalam pengiriman paket.

### 3.10.3. Format *Frame* yang Paling Sering Digunakan

a. *Request To Send (RTS)*



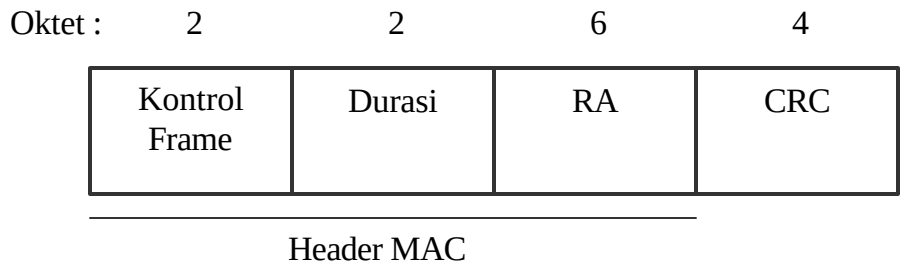

Gambar 3.30. Format *frame RTS*

*Receiver Address (RA)* merupakan alamat dari terminal pada medium nirkabel yang akan menerima *frame* data ataupun *frame* manajemen selanjutnya.

*Transmitter Address (TA)* merupakan alamat dari terminal yang mengirimkan *frame RTS.*

*Duration* berisi nilai waktu dalam mikro detik yang diperlukan untuk transmisi *frame* data maupun *frame* manajemen dengan ditambah satu *frame CTS*, satu *frame ACK,* dan tiga interval *SIFS.*

b. *Clear To Send (CTS)*

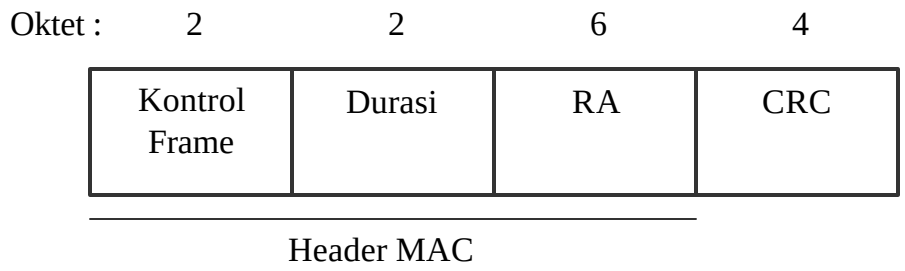



Gambar 3.31. Format *frame CTS*

*CTS* merupakan respon dari *RTS* yang baru saja diterima, dimana *Receiver Address (RA)* pada *CTS* diambil dari bagian *Transmitter Address (TA)* pada *frame RTS.*

Waktu durasi (dalam mikro detik) yang ada didalam *frame CTS* diambil dari bagian *duration RTS* yang diterima dengan dikurangi waktu yang dibutuhkan untuk mentransmisikan *frame CTS* dan interval *SIFS*-nya.

c. *Acknowledge (ACK)*




Gambar 3.32. Format *frame ACK*

*RA* dari *frame ACK* diambil dari bagian alamat kedua pada *frame* yang diterima sebelumnya.

Bila pada *frame* yang diterima sebelumnya bit *More Fragment* nya diset "0" maka bagian duration diset "0", jika tidak maka nilai *duration* diambil dari bagian durasi *frame* yang sebelumnya diterima dikurangi waktu yang dibutuhkan untuk mentransmisikan *frame ACK* dan interval *SIFS* nya (dalam mikro detik).

### 3.11. *Channel Agility*

*Channel Agility* merupakan fungsi tambahan pada standar *802.11b*, fungsi ini digunakan untuk mengatasi beberapa kesulitan pada penggunaan kanal statis seperti *jamming* tanpa membebani fungsi lainnya.

Saat *channel agility* digunakan *layer physical* harus memenuhi syarat pergantian/lompatan kanal dan pewaktuannya. Kemampuan ini pada dasarnya juga dapat digunakan untuk implementasi sistem *802.11b* yang dapat bekerja baik pada teknik *FHSS* maupun *DSSS.*

### 3.12. *Transmit Power*

Energi maksimum yang boleh dikeluarkan oleh peralatan radio diatur oleh badan di masing-masing negara tempatnya beroperasi, yang ditabelkan dibawah ini:

Tabel 3.12. Energi transmisi

| Maximum energi keluaran | Lokasi | Dokumen yang mengatur |
|---|---|---|
| 1000 mW | USA | *FCC* 15.247 |
| 100 mW *(EIRP)* | Eropa | *ETS* 300-328 |
| 10 mW*/MHz* | Jepang | *MPT* ordinance for Regulating Radio Equipment, article 49-20 |

Pengontrolan tenaga harus dilakukan untuk peralatan yang tenaga transmisinya lebih besar dari 100 mW, yaitu maksimum empat tingkatan pengaturan tenaga harus disediakan. Sedangkan minimumnya, radio dengan transmisi melebihi 100 mW harus mampu mengubah energi transmisinya kembali ke 100 mW atau kurang.