# A Brief Tutorial on the PHY and MAC layers of the IEEE 802.11b Standard

Benjamin E. Henty

July 12, 2001

**[This document is a draft version and should not be considered complete. For corrections, questions or comments please contact the author via email at henty+wlan@abtech.org]**

## 1 Organization of the Standard

The IEEE 802.11b standard is broken into two main layers: the MAC or Media Access Control layer and the PHY or Physical Layer. These two layers allow a functional separation of the standard and, more importantly allows a single data protocol to be used with several different RF transmission techniques. Since the goal of this thesis is to predict the performance of IEEE 802.11b wireless LAN products, this chapter will present an overview of the DSSS function of the PHY layer and a basic description of the MAC layer.

## 2 Physical Layer

The PHY layer of the 802.11 standard defines the different RF transmission techniques. There are three basic transmission techniques: Frequency Hopping Spread Spectrum or FHSS, Direct Sequence Spread Spectrum or DSSS, and Diffuse Infrared. The relationship of these three standards is shown in figure 2. Note that the diffuse infrared PHY access technique has received

little attention and will be neglected in this thesis as it is not relevant to the research which has been conducted.

The two remaining PHY access techniques operate in in channels spread between 2.4 and 2.497 GHz. However, the FHSS technique has also been substantially less popular than the DSSS technique. This is mainly due to the higher bandwidth available to the DSSS implementation and the fact that the DSSS function lends itself better to interoperability between different implementations. For this reason, this thesis focuses on the more popular technique of DSSS used under the IEEE 802.11b standard. The specific channels available vary by country and the regulation agencies which controls the spectrum allocation. An description of the spectrum available in different countries is shown in Table 2.

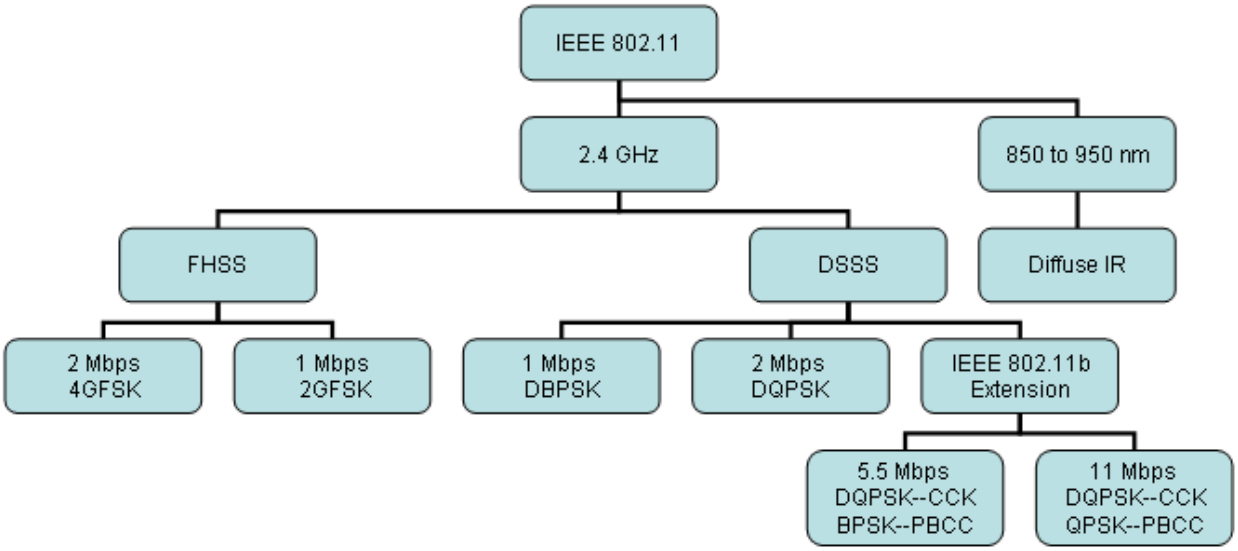


Figure 1: A diagrammatic overview of the IEEE 802.11 standard.

## 2.1 Basic Spreading Technique

Direct Sequence Spread Spectrum uses a PN spreading code to spread transmitted data over a wide bandwidth. This can be thought of as XORing a stream of data bits with a specific PN sequence. In the 802.11 standard, a

Table 1: World Wide Spectrum Allocation for IEEE 802.11 and 802.11b use. [14]

| Country | Regulatory Agency | Frequency Range Available | DSSS Channels Available | FHSS Channels Available |
|---|---|---|---|---|
| United States | FCC | 2.4 to 2.4835 GHz | 1 through 11 | 2 through 80 |
| Canada | IC | 2.4 to 2.4835 GHz | 1 through 11 | 2 through 80 |
| Japan | MKK | 2.4 to 2.497 GHz | 1 through 14 | 2 through 95 |
| France | | 2.4465 to 2.4835 GHz | 10 through 13 | 48 through 82 |
| Spain | | 2.445 to 2.475 GHz | 10 and 11 | 47 through 73 |
| Remainder of Europe | ETSI | 2.4 to 2.4835 GHz | 1 through 13 | 2 through 80 |

single PN code is used by every user in the network. (See Section 3.3 for information about multiple access techniques). This PN code is the 11 bit barker sequence: +1 -1 +1 +1 -1 +1 +1 +1 -1 -1 -1. The technique of XORing data with the Barker sequence is shown in Figure 2.1. The figure shows how a "one" or a "zero" is transmitted as 11 bits of data represented by the original Barker sequence or the inverse of the Barker sequence. By combining data with a bandwidth at baseband of 1 MHz, spreading it and up-converting it to the desired 2.4 GHz channel results in an RF channel bandwidth of 22 MHz, as is shown in Figure 2.1. The channels defined by the IEEE 802.11 standard for different countries are shown in Figure 2.1.

## 2.2 DSSS Advantages

The DSSS technique has two major advantages. It provides a spreading gain against narrowband interference signals and it spreads the transmitted signal across a wide range so the transmission resembles noise to a narrowband receiver. These two characteristics are why DSSS was originally used by the military because it is difficult to jam and difficult to detect by narrowband radios. These two characteristics also make the DSSS technique ideal for coexisting with other narrowband users.

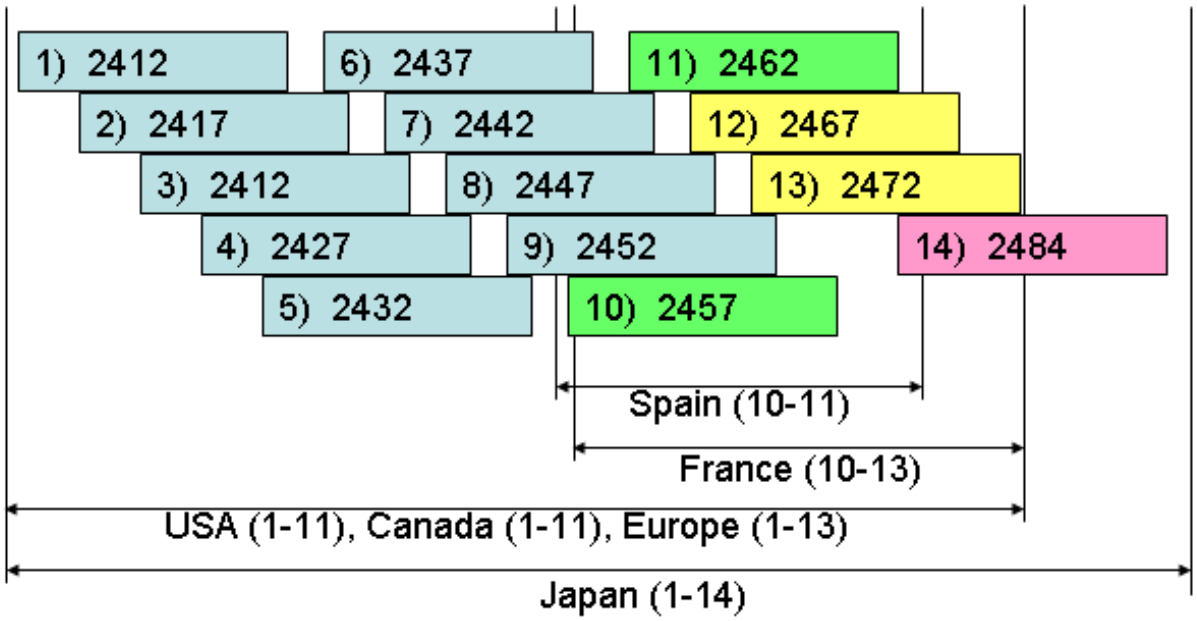


Figure 2: Illustration to scale of IEEE 802.11 DSSS Channels. The channels are labeled by channel number and center frequency, in MHz. Note that channels 12 and 13 are not used in the USA or Canada even though they lie within the allocated frequency bands. Note also that channel 10 is defined for use in France even though it slightly exceeds the valid frequency band available in France. Lastly, also note that channel 14 is slightly offset from the other channels which all have 5 MHz spacings. All Channels have 22 MHz Bandwidths.

## 2.3 Data Bandwidths and Modulation Techniques

DSSS is currently a very popular transmission technique because it has the highest data bandwidth available. The DSSS transmission technique is defined in both the IEEE 802.11 and IEEE 802.11b standard. The 802.11b standard was introduced after the 802.11 standard to define 2 different modulation techniques in addition to the two originally defined in the original 802.11 standard. The original 802.11 standard originally defined two data bandwidths (e.g. bit rates): 2 Mbps and 1 Mbps. These bandwidths use the Barker sequence described above. However, the data is modulated using DQPSK and DBPSK for the 2 Mbps and 1 Mbps bandwidths respectively. The next section discusses the addition of the 5.5 and 11 Mbps bandwidths

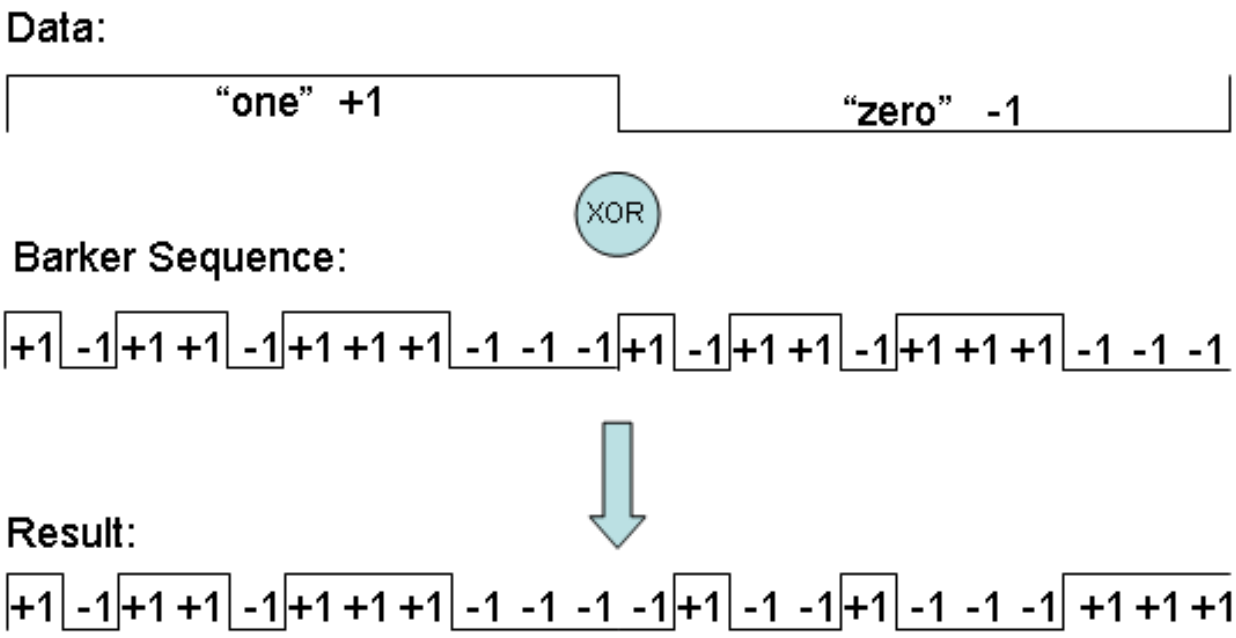


Figure 3: Illustration of the processing spreading data using a Barker Sequence.

to the IEEE 802.11 standard.

## 2.4 IEEE 802.11b Specific Extensions to the DSSS PHY function

The IEEE 802.11b standard defines two additional data bandwidths of 5.5 and 11 Mbps respectively. These new transmission rates also use DQPSK to modulate the data, however the data is no longer spread using the Barker Sequence defined above. In order to increase the data rate to 5.5 and 11 Mbps, the IEEE 802.11b standard uses Complimentary Code Keying (CCK) or optionally Packet Binary Convolutional Coding (PBCC). Both techniques are discussed in the next two sections.

### 2.4.1 CCK Encoding

The IEEE 802.11b standard requires modems to support a technique known as Complementary Code Keying to simultaneous spread data across a 22 MHz channel while transmitting more data bits per 11 spread bits than the 1 or 2

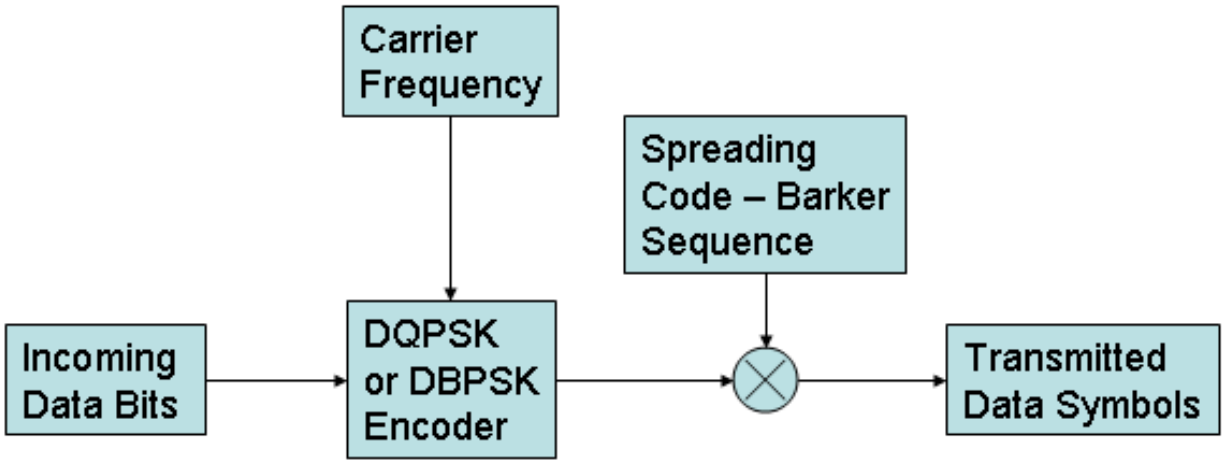


Figure 4: Illustration of the basic IEEE 802.11 Spreading technique

bits transmitted in the plain IEEE 802.11 standard. The 11 Mbps version of CCK encoding works using an 8 chip spreading sequence. This can be done because the 8 bit sequence still runs at a rate of 11 Megachips per second, which results in a spreading factor of 11. CCK encoding, however, does not use a static PN code. It calculates a different spreading code based on the incoming data. This is done by breaking the incoming bits into symbols of 8 bits in duration. An 8 chip spreading code is found from the 8 data bits. Each chip is then encoded using the same DQPSK constellation and then transmitted.

The 11 Mbps CCK technique of calculating the CCK spreading code can be broken down into two steps. First, 8 data bits are split into pairs called dibits. The four dibits are first used to calculate four phase angles, $\varphi_1$ through $\varphi_4$. The 2nd through 4th dibits are converted to a phase angle, $\varphi$ using the mapping shown in Table 2. The first dibit is converted to $\varphi_1$ using Equation 1. That is, $\varphi_1$ found as the value of $\varphi_1$ for the previous symbol plus an offset angle found using Table 2 plus 180 degrees if this is an odd symbol, 0 if it is an even symbol. This results in four phases, $\varphi_1$ through $\varphi_4$.

$$\varphi_1(i) = \varphi_1(i-1) + offset(1stdibit) + \pi * (mod(i,2)) \quad (1)$$

Table 2: Mapping of dibits to Angles for CCK Modulation

| dibit | $\varphi$ value or offset angle, radians |
|---|---|
| 00 | 0 |
| 01 | $\pi/2$ |
| 10 | $\pi$ |
| 11 | $3\pi/2$ |

In the second step the four phases are used to calculate 8 complex chips using the mapping in Table 3. The 8 complex chips are then mapped to the same QPSK constellation and transmitted. Note that the QPSK constellation is actually a DQPSK constellation. The value of $\varphi_1$ offsets all of the chips by the same angle, which is an offset to the QPSK constellation used for the previous set of 8 complex chips.

Table 3: Mapping of Angles into Complex Chips for CCK Modulation

| Chip Number | Formula |
|---|---|
| 0 | $e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi 4)}$ |
| 1 | $e^{j(\varphi_1+\varphi_3+\varphi 4)}$ |
| 2 | $e^{j(\varphi_1+\varphi_2+\varphi 4)}$ |
| 3 | $-e^{j(\varphi_1+\varphi 4)}$ |
| 4 | $e^{j(\varphi_1+\varphi_2+\varphi_3)}$ |
| 5 | $e^{j(\varphi_1+\varphi_3)}$ |
| 6 | $-e^{j(\varphi_1+\varphi_2)}$ |
| 7 | $e^{j\varphi_1}$ |

The 5.5 Mbps version of CCK modulation is carried out in the same manner that the 11 Mbps version is carried out, except that only four bits are encoded per symbol instead of eight. Since, there are only four bits per symbol, the $\varphi$ values are calculated differently. In this case the first dibit is still used to encode $\varphi_1$ in exactly the same manner as before using Equation 1. The remaining $\varphi$ values are calculated based on the 3rd and 4th bits. The formulas for these calculations are given in Equations 2, 3 and 4. Once the $\varphi$ values have been calculated, the chips are calculated and mapped to the QPSK

constellation exactly as was done for the 11 Mbps version of CCK.

$$\varphi_2 = (3rdbit) * \pi + \pi/2 \tag{2}$$

$$\varphi_3 = 0 \tag{3}$$

$$\varphi_4 = (4thbit) * \pi \tag{4}$$

The above process can be thought of in a slightly different manner. Instead of calculating the chips as above, the chips can be thought of as being calculated using the equations shown in Table 3 modified to not include $\varphi_1$. That is, each chip would be a function of just $\varphi_2$, $\varphi_3$, and $\varphi_4$. Then, instead of encoding each chip using QPSK, the entire symbol is encoded using a DQPSK encoding based on the value of $\varphi_1$ as a phase difference from the previously transmitted symbol. Then the symbol is spread using the CCK chips calculated using the modified equations. This alternative way of considering the process is show in block diagram form in Figure 2.4.1.

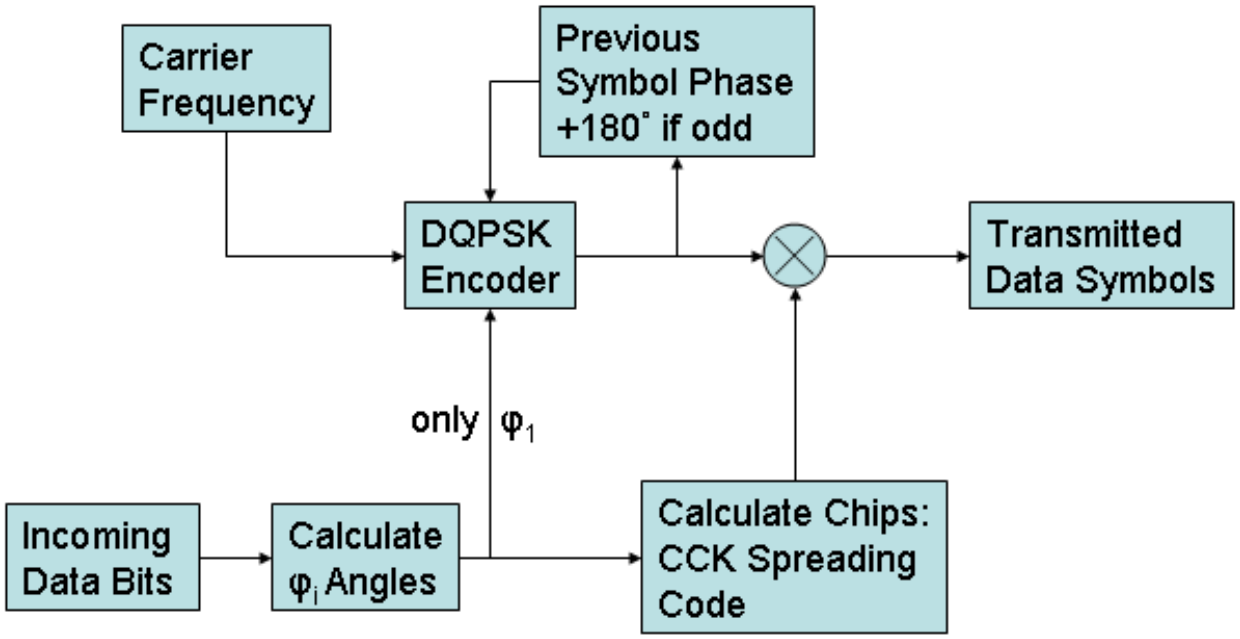


Figure 5: Conceptional block diagram of the CCK encoding process carried out by the transmitter.

To illustrate the CCK spreading process, the sequence 00011011 as an odd

symbol in which the phase of the previous symbol was pi/2 will be encoded. The resulting dibits are 00, 01, 10 and 11. The phases would first be calculated to be $\varphi_1 = \pi/2$, $\varphi_2 = \pi/2$, $\varphi_3 = \pi$, $\varphi_4 = 3\pi/2$. Next, the 8 complex chips would be calculated to be $e^{3j\pi/2}$, $e^{j\pi}$, $e^{j\pi/2}$, $-e^0 = e^{j\pi}$, $e^0$, $e^{3j\pi/2}$, $-e^{j\pi} = e^0$, and $e^{j\pi/2}$. Each chip would be encoded on the QPSK constellation based on the phase of each of the chips.

### 2.4.2 PBCC Encoding

The IEEE 802.11b standard also supports an optional technique known as Packet Binary Convolutional Coding (PBCC) to achieve the 5.5 and 11 Mbps data rates. The PBCC encoding technique uses a standard 1/2 rate, 64 state, rate $\int$ code. The PBCC technique feeds the data bits into the 1/2 rate encoder. The 1/2 rate encoder, by definition, generates 2 output bits for each input data bit. The output of the encoder is mapped to a QPSK constellation for the 11 Mbps data rate and to a BPSK constellation for the 5.5 Mbps data rate. To provide some pseudo-randomness to this technique a pseudo-random cover code is used to vary the QPSK or BPSK constellation used. A block diagram of this technique is shown in Figure 2.4.2

A 256 bit cover sequence is used to vary the QPSK or BPSK constellation used. The cover sequence is generated by taking the 16 bit sequence: 0011 0011 1000 1011 and rotating it 3 bits to the left 15 times to generate the 256 bit sequence made up of 16 sequences of 16 bits each. Thus the 17th through 32nd bits of the full sequence are 1001 1100 0101 1001. The 33rd through 48th bits are 1110 0010 1100 1100. This 256 bit sequence is used repeatedly to vary the constellation used to transmit each chip. Specifically, if the cover sequence is a 0, one constellation is used. If the cover sequence is a 1, then the constellation is rotated by +pi/2 and used. After the end of the 256 bit sequence, the sequence is repeated.

Note that no "spreading" takes place in this technique. Rather, the data is encoded directly at the desired data rate (either 11 Mbps or 5.5 Mbps). However, the use of the cover sequence will act to randomly distribute the data transmission across the full 22 MHz channel bandwidth and the "spreading"

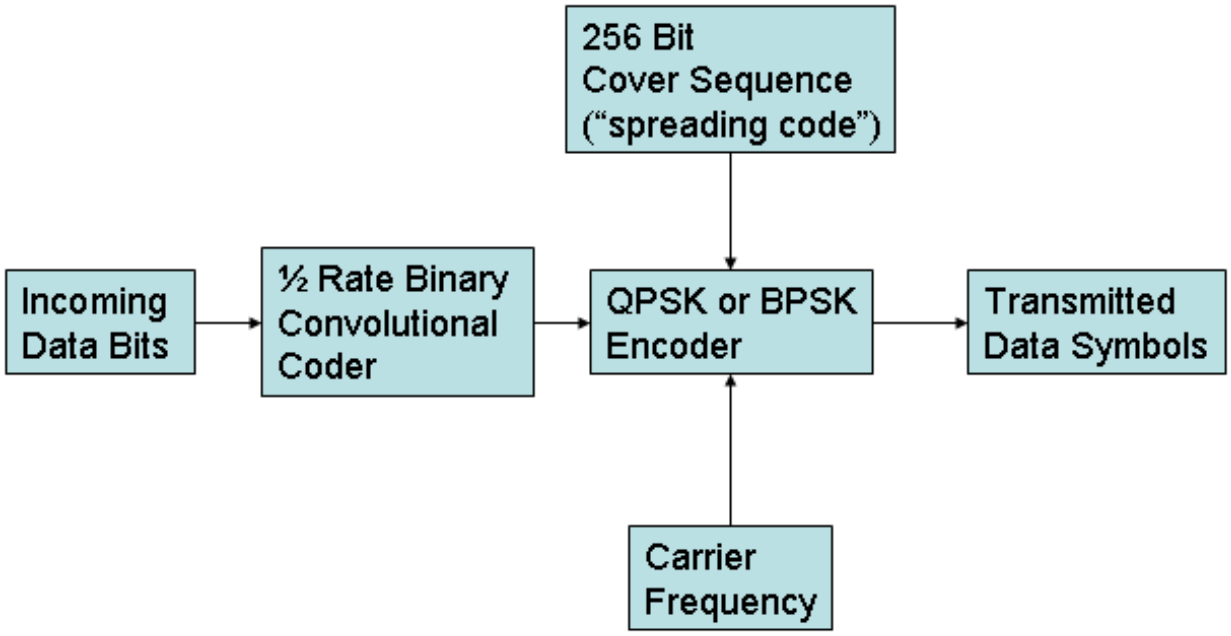


Figure 6: A block diagram of the PBCC encoding technique

can be thought of as occurring inside the QPSK or BPSK encoder.

### 2.4.3 PHY Layer Packet Format

The IEEE 802.11b standard defines two different packet structures that are used in the DSSS standard. There is a short and a long packet format as shown in figure 2.4.3. The short packet format is intended to reduce the overhead of transmissions while the long packet format is to maintain compatibility with IEEE 802.11 networks. The PHY preamble is used to allow the receiver to get synchronized to the transmitter. The PHY header is the overhead needed by the PHY layer. The remainder of the packet contains the data passed to the PHY layer by the MAC layer as is shown in 3.2.

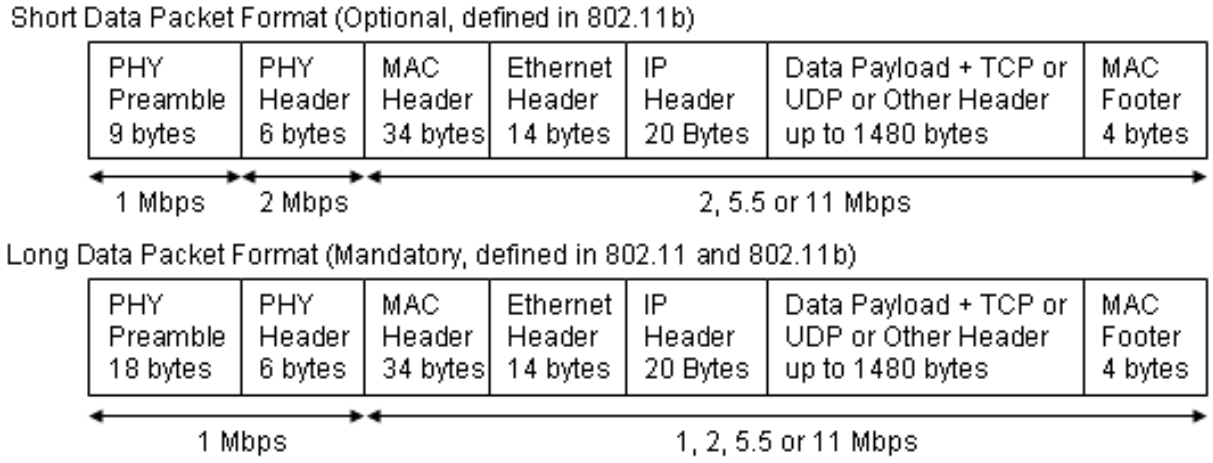


Figure 7: Basic structure of the IEEE 802.11b packet as it's transmitted on the physical layer is shown here

# 3 MAC Layer

## 3.1 Basic Network Layout

The IEEE 802.11 standard defines two types of networks: Adhoc and Infrastructure. Adhoc networks are self-configuring networks between mobile and portable wireless clients. Infrastructure networks use fixed, interconnected access points to provide connectivity to mobile and portable wireless clients. This thesis will focus on infrastructure networks. Since these networks use fixed location access points, it is import to carefully select the locations of these access points. This is the main motivation for this thesis. Infrastructure based wireless networks need to provide some level of service, either in terms of coverage area or in network performance, or in both. However, in order to carefully place the access points which make up a wireless LAN infrastructure, design rules are needed. Prediction models which can be used to design wireless LAN infrastructure networks are presented later in this thesis.

## 3.2 MAC Layer Packet Structure

The basic format of packets passed to the PHY layer from the MAC layer is shown in figure 3.2. Note that this is the basic format for all packets sent by the MAC layer. Some actual packets do not actually contain all of the fields. However, all fields are present in all data packets. Up to four addresses are needed because it is sometimes necessary to identify the address of the access point used by the transmitter or receiver. Thus, if two wireless LAN users are sending packets to one another but each is using a different access point, the 802.11 MAC address of both access points and both clients will be present in the four address fields.


Figure 8: The structure of packet created at the MAC Layer.

## 3.3 Multiple Access, DCF and CSMA/CA

Regardless of the physical layer used, all IEEE 802.11 wireless LAN clients use the same channel to transmit on. This means the standard needs to define a way in which clients know when they can transmit and when they can't. This is handled using several multiple access mechanisms. The most basic of these is the Carrier Sense Multiple Access with Carrier Avoidance (CSMA/CA) mechanism. This mechanism is defined as part of the Distributed Coordination Function (DCF) of the IEEE 802.11b standard. The DCF is the mandatory method by which clients work together and differ access to the medium so that the all users can use the same wireless channel.

CSMA/CA is based on the multiple access technique used in wired Ethernet connections, Carrier Sense Multiple Access with Collision Detection, CSMA/CD. In both types of CSMA users first sense the transmission medium to see if anyone is transmitting just before transmitting a packet of data. This only partially avoids the possibility of packets being transmitted by two users

Table 4: Different Interframe Spacings (IFS)

| Abbreviation | Meaning |
|---|---|
| SIFS | Short Interframe Spacing |
| PIFS | Point Coordination Function (PCF) Interframe Spacing |
| DIFS | Distributed Coordination Function (DCF) Interframe Spacing |
| EIFS | Extended Interframe Spacing |

at the same time. When two or more packets are transmitted simultaneously, or overlapping in time, a "collision" is said to have taken place. In wired Ethernet connections a user is able to detect when a collision has taken place because a network card is setup to be able to transmit and receive on different physical wires that make up the actual Ethernet cable. This is not possible in wireless Ethernet because when a wireless LAN card is transmitting it can not listen to detect if packets collide.

To partially cope with the inability to detect a collision, the IEEE 802.11 standard attempts to avoid collisions using carefully designed waiting periods that allow multiple users to defer access to the shared wireless channel to one another. That is, IEEE 802.11 clients will always ensure a channel has been idle for a certain period of time before transmitting. The process of deciding how long to wait as governed by the basic DCF is illustrated via a flowchart in Figure 9.

The following presents a basic overview of how the DCF progresses.

1. In Figure 9, flow begins at the top left portion of the diagram. When a data packet is ready for transmission, a client will first sense the medium. If it is idle and remains so for a period of time know as the Interframe Spacing (IFS) period, the packet can be immediately transmitted. A standard, unicast packet (called a directed MSDU or MAC Service Data

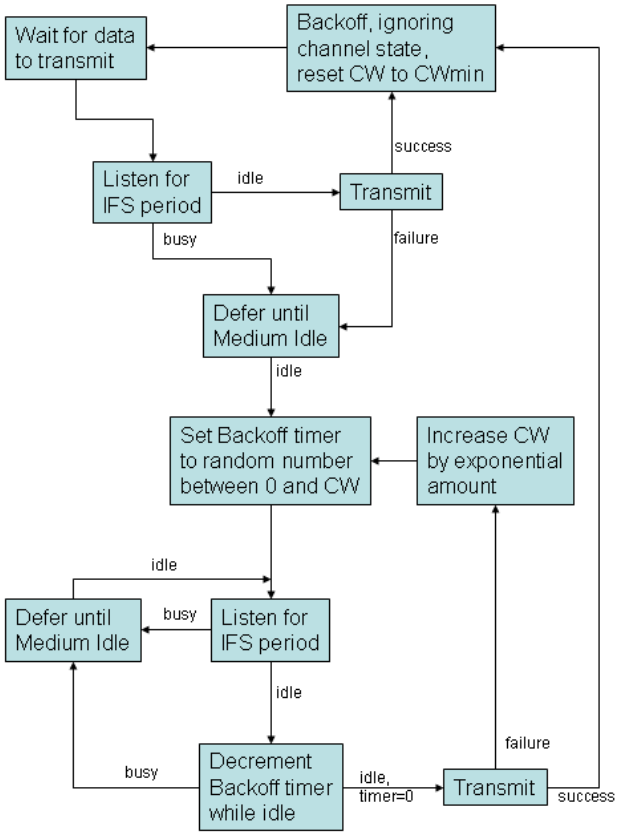


Figure 9: Flow chart of the process of sending data packets under the CSMA/CA based Distributed Coordination Function (DCF).

Unit) needs to be acknowledged by the receiver by a short ACK packet. If this transmission fails by the ACK not being received, the client enters the same defer state as if the medium was initially detected to be busy during the IFS period.

**Note** that their are four different types of IFS frame spacings. These are shown in Table 3.3. The shorter IFS frame spacings are used for higher priority transmissions and to ensure certain events like acknowledgements (ACKs) will occur before another packet transmission.

2. If the medium was not idle or the transmission fails, the client must defer until the medium is free. This is done using a special timer known as

the Network Allocation Vector (NAV). To set this timer the client reads a field in the header of the packet currently being transmitted that tells the client how long the current user will continue to use the medium, through the current transmission, or through the current transmission and immediate transmissions after the current transmission. In this way the client does not need to continue to sense the state of the channel until the NAV timer has expired.

3. After the NAV timer has expired or the client has sensed that the channel is no longer busy, the client will calculate a backoff interval. This backoff interval is a uniform random number. This number is chosen from the interval between 0 and the value of the Contention Window (CW) inclusive. The contention window is initially set to be equal to $CW_{min}$ which is a value defined by the PHY layer.

4. After calculating the value of the backoff interval to use, the senses the channel for an IFS period. If the channel is idle at the end of this period the client will set a backoff timer equal to the value of the backoff period calculated previously. This timer is periodically decremented while the channel continues to stay idle. If the channel becomes busy either during the IFS period or during while the backoff counter is being decremented but before it reaches zero, the client goes into a defer state *without* changing the value of the backoff timer.

5. If the client goes back into a defer state it goes through the same process as before in which the client waits for the medium to become idle by first sensing the medium and then by setting the NAV timer. When the medium returns to an idle state, the client must wait for an additional IFS period before continuing to decrement the backoff counter.

   **Note** that the backoff counter does not get reset to the initially calculated backoff interval each time the client goes into the Defer state. Rather, the backoff counter is decremented whenever the medium has been idle for at least an IFS period.

6. When the medium has been idle for an IFS period and the backoff counter reaches zero, the client will transmit it's data.

7. If the client discovers that the transmission has failed then the client must exponentially increase the value of CW using equation 5. As a result, if the medium is very busy, exponential increases in the maximum backoff delay will occur and the probability of packet collisions will decrease. After increasing CW, the client generates a new value for the backoff interval and re-senses the state of the channel.

8. After either of the two transmit states have been completed successfully (by having been properly acknowledged by the receiver using an ACK packet), several things happen. First, the value of CW is reset to $CW_{min}$ after successful transmission occurs. Second, the client goes through a mandatory backoff interval in which the state of the medium is ignored. The client then goes back to the initial state in which the client waits for data to be ready for transmission.

$$CW_{new} = min(2 * (CW_{old} + 1) - 1, CW_{max}) \tag{5}$$

### 3.4 RTS/CTS and the Hidden Terminal Problem

The DCF implementation of IEEE 802.11 does not handle a problem referred to as the hidden terminal problem. This problem occurs when a mutual receiver is in range of two transmitters which are not in range of one another. In this case attempting to detect if the medium is free does not necessarily work because the two transmitters can not detect one another's transmissions. Thus the packets from the two transmitters will collide at the common receiver. To combat this problem, IEEE 802.11 adds an optional RTS/CTS mechanism. In this technique instead of transmitting a data packet after waiting for a free medium, a client will transmit a short Ready To Send (RTS) packet to request the use of the medium. If this succeeds, the receiver will quickly (after a SIFS period) reply with a short Clear To Send (CTS). After the successful exchange of an RTS/CTS pair the actual transmission takes place. This method allows hidden terminals to hear either a CTS or an RTS packet and know to differ access using the NAV functionality described previously. It also means that if packets do collide only a short RTS

or CTS packet is lost rather than a long data packet. It is important to note though that this functional is optional to include and is enabled in one of three modes: always on, always off or on for packet sizes above a certain threshold.

## 3.5 Additional Optional Provisions of the MAC Layer

### 3.5.1 The Point Coordination Function

Another optional protocol that is part of the IEEE 802.11 standard is the Point Coordination Function (PCF). This function allows time critical or delay sensitive packets to be given priority over regular data transmissions. The PCF uses a polling procedure to setup a contention free period which takes priority over the DCF procedure. During the PCF established contention free period, a single host poles clients and allows them to transmit. In this way delay sensitive packets such as voice or video can be given priority over other data.

### 3.5.2 Wired Equivalent Privacy

The Wired Equivalent Protocol (WEP) is intended to provide a simple layer of protection for wireless network connections. By their very nature, wireless networks are easy to connect to and be eavesdropped on. WEP is a single shared key system in which a basic 40 bit encryption is applied to packet transmissions on the network. Without knowledge of the WEP key, packets can not easily be decoded by an unauthorized user. The use of WEP though tends to slow down transmissions and increases the overhead of packet transmissions, thereby lowering the bandwidth available. In addition, several security flaws have been found in the technique [21].

## References

[1] Pulse Propagation Characteristics At 2.4 GHz Inside Buildings, Seong-Cheol Kim; Bertoni, H.L.; Stern, M., IEEE Transactions on Vehicular Technology, Volume: 45 Issue: 3 , Aug. 1996, Page(s): 579 -592

[2] Hope, M. and Linge, N., "Determining the Propagation Range of IEEE 802.11 Radio LAN's for Outdoor Applications," Local Computer Networks, 1999. LCN '99. Conference on , 1999.

[3] Duchamp, D., and Reynolds, N. F., "Measured Performance of a Wireless LAN," Local Computer Networks, 1992. Proceedings., 17th Conference on , 1992.

[4] "Measured Performance of the IEEE 802.11 Wireless LAN," Local Computer Networks, 1999. LCN '99. Conference on , 1999.

[5] Internet Protocol Performance Over Networks With Wireless Links, Xylomenos, G.; Polyzos, G.C., IEEE Network, Vol. 13 Issue 4: July-Aug 1999 p. 55-63

[6] TCP And UDP Performance Over A Wireless LAN, Xylomenos, G.; Polyzos, G.C., INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE , Volume: 2 , 1999 Page(s): 439 -446 vol.2

[7] Maeda, Y., Takaya, K., and Kuwabara, N., "Experimental Investigation of Propagation Characteristics of 2.4 GHz ISM-Band Wireless LAN in Various Indoor Environments," IEICE Transactions in Communications, Vol. E82-B, No. 10 Oct 1999

[8] Demir T., Komar C., Ersoy C.., Measured Performance of an IEEE802.11 Wireless LAN, Proceedings of the Fifteenth International Symposium on Computer and Information Sciences, pp.246-254, Istanbul/Turkey, October, 2000. ISCIS XV International Symposium on Computer and Information Sciences October 11-13, 2000 Istanbul, Turkey

[9] Kamerman, A.; Aben, G. "Throughput performance of wireless LANs operating at 2.4 and 5 GHz" Personal, Indoor and Mobile Radio Communications, 2000. PIMRC 2000. The 11th IEEE International Symposium on , Volume: 1 , 2000 Page(s): 190 -195 vol.1

[10] Tarng, J. H., Liu, T. R. Effective Models in Evaluating Radio Coverage on Single Floors of Multifloor Buildings IEEE Transactions on Vehicular Technology, Vol 48, No 3, May 1999.

[11] Experimental And Theoretical Evaluation Of Interference Characteristics Between 2.4-GHz ISM-Band Wireless LANs, Takaya, K.; Maeda, Y.; Kuwabara, N., 1998 IEEE International Symposium on Electromagnetic Compatibility, 1998., Volume: 1, Page(s): 80 -85 vol.1

[12] Prasad, A.R.; Prasad, N.R.; Kamerman, A.; Moelard, H.; Eikelenboom, A., "Indoor Wireless Lans Deployment" Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st, Vol. 2, 2000 p. 1562-1566 vol. 2

[13] Optimal prediction tool for wireless LAN using genetic algorithm and neural network concept Shih-An Chen; Yang-Han Lee; Yen, R.Y.; Yu-Jie Zheng; Chih-Hui Ko; Shiann-Tsong Sheu; Meng-Hong Chen Communications, 1999. APCC/OECC '99. Fifth Asia-Pacific Conference on ... and Fourth Optoelectronics and Communications Conference , 1999 Page(s): 786 -789 vol.1

[14] IEEE 802.11 Standard

[15] N. R. Prasad. "IEEE 802.11 System Design" Personal Wireless communications, 2000 IEEE International conference on, 2000 p. 490-494

[16] Experimental Investigation Of Controlling Coverage Of Wireless LAN By Using Partitions With Absorbing Board, Maeda, Y.; Takaya, K.; Kuwabara, N. Electromagnetic Compatibility, 1999, International Symposium on , 1999 Page(s): 674 -677.

[17] S.-H. Yang et al. "A Wireless LAN Measurement Method Based on RSSI and FER"

[18] A. Messier, J. Robinson, K. Pahlavan. "Performance Monitoring of a Campus Area Network." 1997.

[19] D. Leskaroski, W. B. Mikael. "Frequency Planning and Adjacent Channel Interference in a DSSS Wireless Local Area Network"

[20] http://www.netiq.com/Products/Network_Performance/Chariot/Default.asp. "NetIQ Products - Chariot" Viewed: June 14, 2001

[21] Nikita Borisov, Ian Goldberg, and David Wagner. "(In)Security of the WEP algorithm." http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html Viewed: July 4, 2001